ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5

Maintenance Report Number: CCEVS-VR-VID10337-2011a

Date of Activity: 11 October 2011

References: **"**Common Criteria Evaluation and Validation Scheme, Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation"

"McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5 Impact Analysis Report, May 31, 2011"

Documentation Updated: McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5 evidence documents.

Assurance Continuity Maintenance Report:

On 6 June 2011, McAfee, Inc., submitted an Impact Analysis Report (IAR) to CCEVS for approval. The IAR is intended to satisfy requirements outlined in **"**Common Criteria Evaluation and Validation Scheme, Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, 8 September 2008, Version 2.0". 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 maintenance activity covers patches and updates to the McAfee Policy Auditor 5.2 and ePolicy Orchestrator 4.5 (validated Target of Evaluation (TOE)) to McAfee Policy Auditor 5.3 and ePolicy Orchestrator 4.5 ("maintenance evaluation").

The product changes in the maintenance evaluation include the following:

- Enhanced, actionable findings
- Per audit data maintenance
- Removal of empty or erroneous content and benchmarks
- Support for additional operating systems
- Targeted content distribution
- OVAL 5.6 compatibility and support
- Version control and content tracking of text files
- Conditional Checks for Effective Rights
- Joint McAfee Policy Auditor and McAfee Integrity Manager dashboard and reports
- Rollup reporting

The changes were related to availability or performance of the TOE in general, which do not correspond to any Security Functions (and have no relation to any Security Functional Requirements (SFRs)), and hence were considered to be out of scope when compared to the original evaluation. The changes regarding management actions are extensions of existing functionality and are too granular to be considered a substantial change, since the core functionality and architecture remains the same.

Analysis and Testing:

All the fixes were built into and tested with the product prior to its release. This helped to ensure that there were no adverse effects resulting from the changes.

Conclusion:

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 original assurance is maintained for the above-cited versions of the product.