CCEVS Approved Assurance Continuity Maintenance Report

VID#:   **10292**

Product Name: Boeing Secure Network Server (SNS)
EAL: EAL5+
Date of Activity: 2013-08-29

References: Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) Security Target, Version 2.5, 2/3/2011.

SNS EAL5+ Assurance Continuity Impact Analysis Report (IAR); Boeing Document Number D950-11204-1, Rev A.

Documentation Updated:

Trusted Facility Manual updated to reflect the revised software version 3.10.9.

I.   Introduction

In April 2013 Boeing submitted an Impact Analysis Report (IAR) for the Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) to the CCEVS for review. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme - Assurance Continuity: Guidance for Maintenance and Re-evaluation, Version 2.0, September 8, 2008. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the Boeing Secure Network Server (SNS), the evidence updated as a result of the changes and the security impact of the changes

II. Changes to the TOE

a. Hardware Changes

In order to address hardware obsolescence issues with the existing hardware base, three (3) new hardware elements were substituted in the TOE;

- Disk on Module (DOM)
- Optical Disk Drive (i.e., DVD)
- Solid State Drive

See details in Section 2.1 of the IAR.

b. Software/ Firmware Changes

- Correction for a filesystem implementation error in audit trail archiving; added a check for the size of the output audit record block to be written to the CD archive

backup on optical disk media, to ensure it exactly matches the size of the audit record.

- Interface logic for substitute Disk on Module (DOM);
- Interface logic for substitute Optical Drive; introduce a one-second delay in the initialization sequence in the optical disk code to accommodate a slight difference in start-up timing in the new part;
- Incorporate substitute Solid State Drive.

The details are presented in Section 2.2 of the vendor's IAR

All software and firmware changes were deemed to be Minor. None of the changes affect the TSF user interface or the enforcement of security policy. Testing was performed to verify the TOE functions as specified.

No Major defects were found, either in hardware, firmware, or software.

c. *Vendor Processes*

All changes were processed through the Boeing Engineering Change Board (ECB). Testing was performed and validated by Boeing QA.

Code tests performed to verify continued hardware/firmware/software compatibility and interoperability across the SNS models.

In addition to developer unit testing of code changes for each Software Problem Report (SPR), the entire set of test procedures used in the original evaluation of TOE version 3.10.7 were repeated on the integrated TOE version 3.10.9 after all developer changes were complete and approved. Test related procedures, report, and log files were captured as test evidence and placed into controlled archives.

Covert channel analysis was re-visited, and *Minor* test procedure modifications were implemented to account for the speed changes exhibited by the upgraded hardware. Each hardware behavior change was analyzed to ensure continued compliance with requirements and assurance. Variances in throughput and response times were found to remain within tolerances for performance and covert channels.

III. Conclusion

This maintenance activity covers the assessment of the evaluation impact of the changes applied to Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210).

The conclusion of the CCEVS is that the original assurance rating granted has been maintained for the above version of the product