# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme


TM

# Validation Report

# Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210)

**Report Number: CCEVS-VR-VID10292-2011**
**Dated: 18 April 2011**
**Version: 1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6940**
**Fort George G. Meade, MD 20755-6940**

# ACKNOWLEDGEMENTS


**Validation Team**

Ken Elliott
Aerospace Corporation

Shaun Gilmore
NIAP CCEVS

**Common Criteria Testing Laboratory**

*Science Applications International Corporation*
*Columbia, Maryland*

# Table of Contents

# 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) (henceforth referred to as SNS). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in May 2007. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria version 2.3, Part 2 Conformant and Part 3 Conformant**, and meets the assurance requirements of EAL 5 augmented with ACM_AUT.2, ACM_CAP.5, ADO_DEL.3, ADV_HLD.4, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ALC_DVS.2, ALC_FLR.2, ALC_LCD.3, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2, AVA_CCA.2, and AVA_MSU.3.

The Target of Evaluation (TOE) is Boeing Secure Network Server (SNS), versions 3010, 3110, and 3210. Each version of the TOE utilizes the same software and bios; the primary differences being physical. The 3010 version includes a 4U rack-mountable chassis and the 3210 version includes a 2U rack-mountable chassis. The 3110 version includes a 2U flight-worthy chassis that, unlike the other two versions, utilizes a solid-state hard drive. It is capable of controlling information flows based on information in packet headers, packet contents, and security labels associated with packets and the subscribers. Each subscriber is configured with a sensitivity label range that limits (via Mandatory Access Controls (MAC)) the labels that can be associated with information that can come from or go to a given subscriber. In addition to MAC, the SNS can be configured to limit the flow of information based on packet attributes (e.g., addresses), contents, and other datagram characteristics as well as to constrain the flow of information to mitigate the potential for covert channels. The information flow policies are managed by defined administrators that can manage subscriber devices and the policy rules to affect an information flow policy suitable for their specific application.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation

team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for EAL 5 augmented with ACM_AUT.2, ACM_CAP.5, ADO_DEL.3, ADV_HLD.4, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ALC_DVS.2, ALC_FLR.2, ALC_LCD.3, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2, AVA_CCA.2, and AVA_MSU.3 have been met. The Embedded OS Team in the Operating Systems and Embedded Technology Division and the Enterprise Application Division at NSA augmented the evaluation by performing an examination of evidence, vulnerability analysis, and penetration testing for the requirements in AVA_CCA.2 and AVA_VLA.3.

# 2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for EAL 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

**Table 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| **Evaluated Product:** | Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) |
| **TOE Identification:** | Boeing SNS-3010, SNS-3110, SNS-3210<br>Boeing SNS Custom Transaction Kernel<br>Secure Network Server COTS Hardware<br>Custom BIOS |
| **Sponsor & Developer:** | The Boeing Company<br>P.O. Box 3999, M/S 88-12<br>Seattle, Washington 98124-2499 |
| **Common Criteria Testing Lab (CCTL):** | Science Applications International Corporation,<br>Common Criteria Testing Laboratory<br>7125 Columbia Gateway Drive, Suite 300<br>Columbia, MD 21046 |
| **Validation Team:** | Ken Elliott, Aerospace Corporation<br>Shaun Gilmore, NIAP CCEVS |
| **Protection Profile:** | None |
| **ST Title:** | Boeing Secure Network Server (SNS-3010, SNS-3110 and SNS-3210) Security Target, Version 2.5, 2/3/2011 |
| **CC Version:** | Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005 |
| **Conformance Claims:** | Common Criteria for Information Technology Security Evaluation Part 2 conformant<br>Common Criteria for Information Technology Security Evaluation Part 3 conformant |
| **Assurance Level:** | EAL 5 augmented with ACM_AUT.2, ACM_CAP.5, ADO_DEL.3, ADV_HLD.4, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ALC_DVS.2, ALC_FLR.2, ALC_LCD.3, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2, AVA_CCA.2, and AVA_MSU.3 |

# 3 Security Policy

The Security Functional Policies (SFPs) implemented by Boeing SNS are based upon the basic set of security policies that include policies that permit protection of user data, provide for authenticated user access, provide accountability for actions, and protect the mechanism that provides the security policies.

Note: Much of the description of the Boeing SNS security policy has been extracted and reworked from the Boeing SNS Security Target.

## 3.1 Security Audit

The Boeing SNS generates audit events for security relevant events, including covert channel indicators. The audit events are stored and protected, and forwarded to the NM for review and archival purposes. The SNS sends warning when the audit storage capacity is nearing or has exceeded its capacity and it can be configured to automatically overwrite events or to stop operations altogether until the situation is remedied.

## 3.2 User Data Protection

The Boeing SNS is designed primarily to control the flow of information between subscriber devices. It enforces a rich set of information flow policies including mandatory access controls based on subscriber sensitivity labels, packet filtering, and content filtering. It also provides routing and processing functionality to offer static routing, multicast support, and ICMP.

## 3.3 Identification and Authentication

While all users (administrators) and subscriber devices are identified by the SNS, it also requires that administrators are authenticated at an appropriate management console prior to offering management functions. This is accomplished by managing user definitions, including user identities, roles, and associated authentication data (i.e., passwords).

In order to help mitigate attempts to bypass the authentication mechanisms, the Boeing SNS informs users each time they log in of the last time they successfully logged in, the number of unsuccessful logins that have occurred since the last successful login, and the time of the last unsuccessful login attempt.

## 3.4 Security Management

The Boeing SNS offers command line interfaces for the management of the TOE Security Functions. There are three defined roles: Network Administrator (NA), Security Administrator (SA), and Super-SA. The Super-SA primarily manages the administrator accounts, the SA primarily manages the security functions, and the NA primarily manages the general operational capabilities of the TOE. Each administrator must log into the appropriate console before applicable functions can be accessed.

## 3.5 Protection of the TOE Security Functions

The Boeing SNS is designed around a custom operating kernel that makes use of the ring architecture offered by Intel Pentium 4 processors to protect itself and to separate itself to implement a least privilege principle. All traffic flowing through the TOE is subject to its

security policies. Furthermore, the TOE includes self tests that run at initial start-up and also periodically when the TOE is operational. The TOE also includes failure detection and recovery features to ensure that it continues to operate correctly when recoverable failures occur and to ensure that it shuts down when necessary when manual recovery becomes necessary.

The Boeing SNS is designed so that a given part of a distributed SNS system can continue to operate properly when some other system components (i.e., other SNSs) fail. It is also designed to limit the throughput of a given device to protect itself and other network components as may be necessary.

# 4 Security Environment

## 4.1 Threats

| | |
|---|---|
| T.AUDIT | Attempts to violate TOE security policies may go undetected or users may not be accountable for security-relevant actions they perform. |
| T.FILTER | Inappropriate network traffic may enter or leave a protected network. |
| T.I&A | Unauthorized users may be able to inappropriately configure the TOE or access sensitive TOE data. |
| T.MAC | Classified information may be inappropriately accessed by entities that do not have appropriate clearances. |
| T.OPERATE | The TOE may fail to provide or enforce its security functions due to failure or malicious attacks against its security mechanisms. |

## 4.2 Assumptions

| | |
|---|---|
| A.ADMIN | The TOE administrators are competent, adhere to the applicable guidance, and are not willfully negligent or malicious. |
| A.COMMS | The TOE is able to communicate with its attached subscriber devices. |
| A.FLOW | Protected information does not flow among the network subscribers unless it passes through the TOE. |
| A.PHYSEC | The TOE is physically secure; specifically it, including the communication media among distributed parts of the TOE, is protected from physical tampering of itself or its physical connections to its environment (subscriber devices). |
| A.SUBSCRIBE | A process outside the scope or control of the TOE is used to determine the attributes (e.g., sensitivity ranges) of attached subscriber devices. |

## 4.3 Security Objectives for the TOE

The security requirements enforced by the TOE were designed based on the following overarching security policies:

| | |
|---|---|
| O.AUDLOS | The TSF shall be configurable to limit the potential loss of audit information. |

| | |
|---|---|
| O.AUDREC | The TOE shall provide a means to record an audit trail of security-related events, with accurate dates and times. |
| O.AUDREV | The TSF shall protect the audit trail so that only an authorized administrator can access the audit trail. |
| O.AUDTHR | The TSF shall allow audit thresholds to be defined that will trigger alarms when attempted policy violations exceed the defined thresholds. |
| O.FILTER1 | The TOE shall allow (only) an authorized administrator to explicitly define information filtering rules. |
| O.FILTER2 | The TOE shall restrict the flow of information among subscriber devices based on filtering rules based on information headers and content established by the authorized administrator. |
| O.IDAUTH | The TOE shall uniquely identify and authenticate the claimed identity of all administrators before granting access to TOE functions related to the assumed administrator role. |
| O.IMPEXP | The TOE shall import and export labeled and unlabelled data according to the sensitivity labels associated with attached subscriber devices. |
| O.MAC1 | The TOE shall allow (only) an authorized administrator to assign sensitivity labels to subscriber devices. |
| O.MAC2 | The TOE shall restrict the flow of information between attached subscriber devices so that information from one subscriber can be sent to another subscriber only if the sensitivity level of the information is within the range of sensitivity labels the receiving subscriber device is allowed to process. |
| O.PROTECT | The TOE shall ensure that its functions are always invoked and that it is resistant to potential attacks against its security functions. |
| O.RECOVER | The TOE shall secure and be able to recover from failure conditions and will continue to operate when possible. |
| O.SELFTEST | The TOE shall test its own operation in order to detect potential failures. |

## 4.4 Security Objectives for the Environment

| | |
|---|---|
| OE.ADMIN | The TOE administrators will be competent, adhere to the applicable guidance, and will not be willfully negligent or malicious. |
| OE.COMMS | The TOE will be able to communicate with its attached subscriber devices. |
| OE.FLOW | Protected information does not flow among the network subscribers unless it passes through the TOE. |
| OE.PHYSEC | The TOE, and the communication media among distributed parts of the TOE, will be physically protected from physical tampering of itself or its physical connections to its environment. |
| OE.SUBSCRIBE | A process outside the scope or control of the TOE will be used to determine the attributes (i.e., sensitivity ranges) of attached subscriber devices. |

# 5 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Boeing SNS is a network appliance running on a custom kernel that runs on COTS hardware (with a custom BIOS) based on the Intel Pentium 4 processor. The SNS utilizes the Intel Pentium 4 ring architecture to separate its own functions resulting in a well-layered design that implements a least privilege principle. Each appliance supports serial devices (management consoles) and network devices (subscriber devices).

The TOE consists of hardware and firmware, composing one or more Boeing SNS appliances with one acting as a Network Management (NM) appliance. The distributed TOE components are always synchronized with the NM and are managed from the central NM appliance. Also, the connections among the distributed TOE components must be distinct from the connections to the subscriber devices since the entire connection media must be protected to protect sensitive TOE communications. The TOE boundary is everything inside the NTCB as shown in Figure 2.

Physically, there may be three consoles (connected via serial ports): utility, SA, and NA. Alternately, a single console (or attached keyboard and monitor) can be configured with control keys used to logically switch between three consoles. The other important interfaces are a dedicated Ethernet port for SNS-to-SNS communication and additional Ethernet ports to the subscriber devices outside the TOE. The consoles offer management functions and the subscriber interfaces internal to the TOE offer controlled information flow among the attached subscriber devices outside the TOE. Figure 1 shows a sample SNS configuration. Figure 2 shows the major architectural components and the TOE boundary.

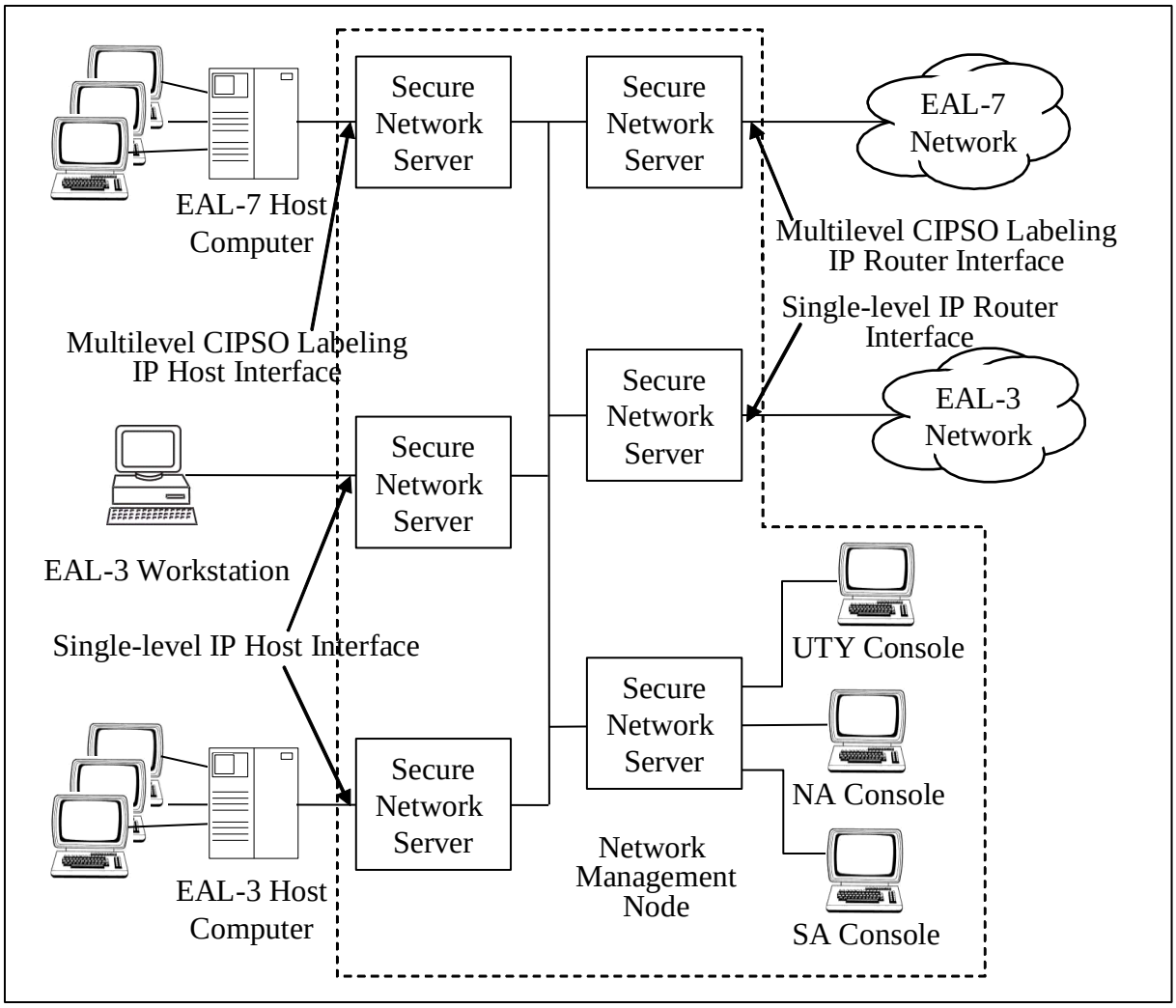


**Figure 1 Sample SNS Configuration**

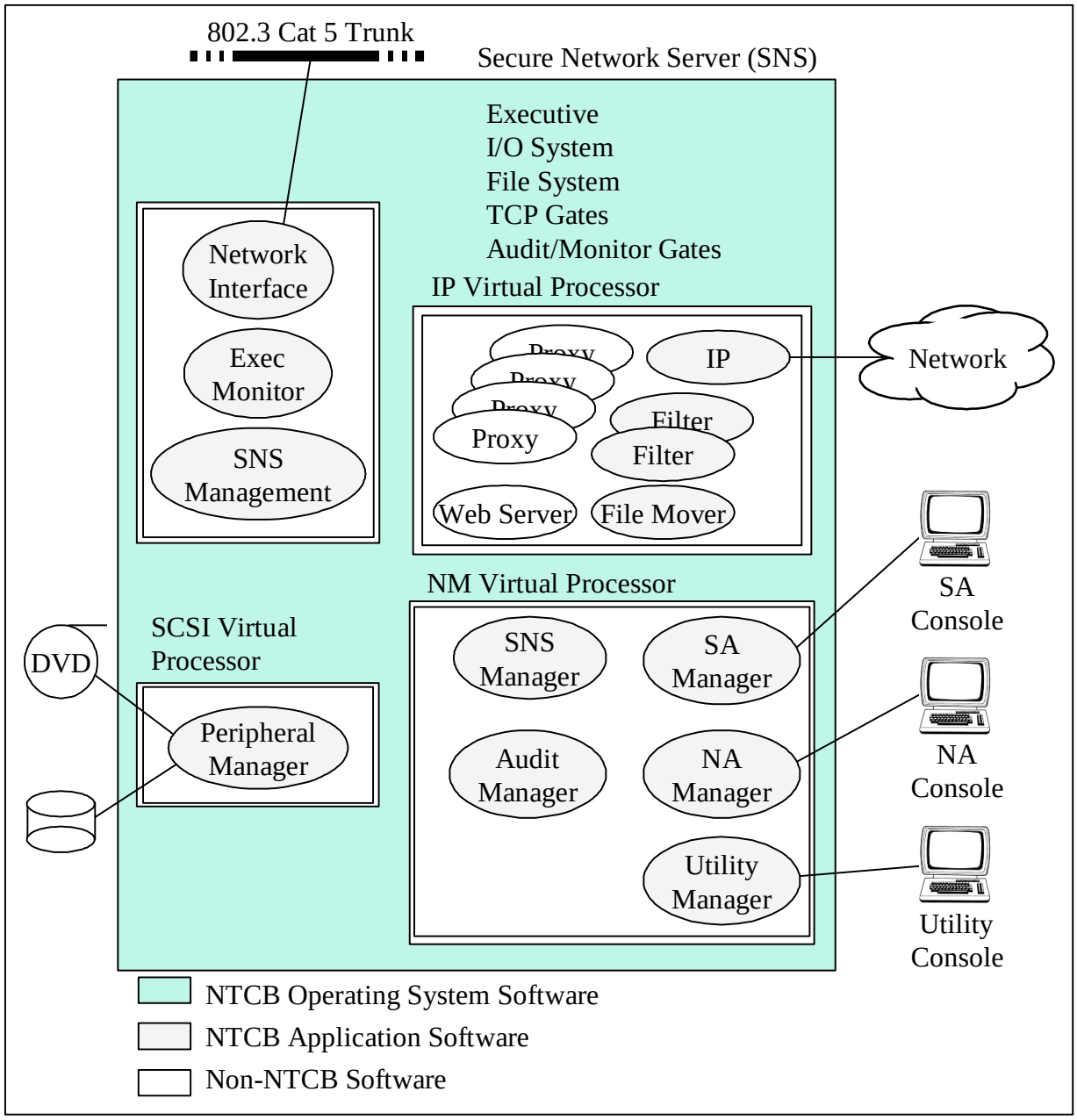


**Figure 2 System Components**

# 6 Documentation

The following documentation was used as evidence for the evaluation of the Boeing SNS:[1]

| Assurance Class | Document Title |
|---|---|
| ASE | • Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) Security Target, Version 2.5, 2/3/2011 |
| ACM | • Boeing SNS Configuration Management Plan, D658-10972-1<br>• Rating Maintenance Plan, D658-10971-1<br>• Boeing SNS Configuration Item List SNS-3010/3110,/3210, 900-18729<br>• Indentured System List, Secure Network Server, 900-18724 |
| ADO | • Boeing SNS Operation and Maintenance Manual, SNS – 3010/3110,/3210, D658-10984-1<br>• Trusted Facility Manual, SNS – 3010/3110,/3210, D658-10974-1 |
| ADV | • Formal Specification, Multilevel Secure Local Area Network, D658-10983-1<br>• Interface Design Description Document, SNS – 3010/3110,/3210, D658-10988-1<br>• Secure Network Server Security Design Concepts, D658-10976-1<br>• SNS–3x10 Requirements Mappings for ADV FSP.2, version 1, November 1, 2006<br>• Hardware Requirements Specification, SNS – 3010/3110/3210, D658-10975-1<br>• Boeing SNS Source Code |
| AGD | • Boeing SNS Trusted Facility Manual, SNS – 3010/3110/3210, D658-10974-1<br>• Security Features User's Guide, SNS – 3010/3110/3210, D658-10973-1 |
| ALC | • Boeing SNS Lifecycle Model, SNS – 3010/3110/3210, D658-10991-1<br>• Boeing SNS Development Environment Protection, SNS – 3010/3110/3210, D658-10989-1<br>• Boeing Configuration Management Plan, D658-10972-1<br>• SNS Life-Cycle Definition, Version 1.0, December 9, 2006<br>• Trusted Facility Manual, SNS – 3010/3110/3210, D658-10974-1 |
| ATE | • Boeing SNS Test Plan, SNS – 3010/3110/3210, D658-10977-1<br>• Boeing SNS Test Procedures, SNS – 3010/3110/3210, D658-10978-1<br>• Boeing SNS Test Coverage and Depth Analysis<br>• Test Report, SNS – 3010/3110/3210, D658-10979-1<br>• Actual Test Results |
| AVA | • Boeing SNS Penetration Test Plan, Section 4, Vulnerability Analysis<br>• Boeing SNS Covert Channel Analysis<br>• Misuse Analysis, SNS-3010/3110/3210, D658-10992-1<br>• Strength of Function Analysis, SNS – 3010/3110/3210, D658-10990-1<br>• Pen Test Plan/Report, SNS – 3010/3110/3020 EAL 5, D658-10980-2 |

[1] This documentation list is based on the list provided in the Evaluation Technical Report, Part 1, developed by SAIC.

# 7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Plan for the Boeing SNS Product, Version 1.0, 8 January 2007.

## 7.1 Developer Testing

At EAL 5, testing must demonstrate correspondence between the tests and the functional specification and high level design. The vendor testing was extensive and covered all of the security functions identified in the ST and interfaces identified in the design. These security functions include:

- Identification and Authentication
- User Data Protection
- Security Audit
- Security Management
- Protection of the TSF

The developer also performed a vulnerability analysis of the product. Boeing performed a search of all public domain sources for known vulnerabilities and performed a flaw hypothesis strategy to identify potential product vulnerabilities. No residual vulnerabilities remain in the product.

## 7.2 Evaluation Team Independent Testing

The evaluation team verified that the TOE was installed as is specified in the secure installation procedures, reran all developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality. The team performed twelve team tests that addressed audit, user data protection, identification and authentication, security management, and resource utilization. In addition to team testing, the evaluation team performed seven penetration tests focused around self-protection, network interface attacks, and password attacks.

## 7.3 Highly Resistant Vulnerability Analysis

Evaluation team testing at NSA was completed in November 2010. Using the results of the evaluation by the CCTL evaluation team, the NSA evaluation team installed the TOE evaluated configuration and conducted AVA_CCA.2 and AVA_VLA.3 vulnerability testing. The NSA team utilized the same category of tools used by the CCTL for penetration testing, as well as in-house developed tools, which enabled the team to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

# 8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210). The product must be installed in its evaluated configuration identified in:

- Operation and Maintenance Manual, SNS – 3010/3110/3210, Document Number D658-10984-1
- Trusted Facility Manual, SNS – 3010/3110/3210, Document number D658-10974-1

# 9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL 5 augmented with ACM_AUT.2, ACM_CAP.5, ADO_DEL.3, ADV_HLD.4, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ALC_DVS.2, ALC_FLR.2, ALC_LCD.3, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2, AVA_CCA.2, and AVA_MSU.3 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3] and CEM version 1.0 [5], [6]. The evaluation determined the Boeing SNS TOE to be Part 2 conformant and to meet the Part 3 EAL 5 augmented with ACM_AUT.2, ACM_CAP.5, ADO_DEL.3, ADV_HLD.4, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ALC_DVS.2, ALC_FLR.2, ALC_LCD.3, ALC_TAT.3, ATE_COV.3, ATE_DPT.3, ATE_FUN.2, AVA_CCA.2, and AVA_MSU.3.

## Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Boeing SNS product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.1 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 5 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to

accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Boeing and performed a CM audit.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.2 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 5 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The Validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.3 Evaluation of the Development (ADV)

The evaluation team applied each EAL 5 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

Additionally, the evaluation team ensured that the security policy model document clearly describes the security policy rules that were found to be consistent with the design documentation.

The Validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.4 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 5 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.5 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 5 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE.

In addition to the EAL 5 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.6 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 5 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions and TSFI as described in the functional specification and high level design specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.7 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 5 AVA CEM work unit. The evaluation team ensured that the TOE did not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The Embedded OS Team in the Operating Systems and Embedded Technology Division and the Enterprise Application Division at NSA augmented the evaluation by performing an examination of evidence, vulnerability analysis, and penetration testing for the requirements in AVA_CCA.2 and AVA_VLA.3.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.8 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

# 10 Validator Comments/Recommendations

The Validation Team observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation Team agrees that the CCTL presented appropriate rationales to support the results and conclusions presented in the *Evaluation Technical Report for Boeing Secure Network Server, Part 2 Version 3.0, April 20, 2007*.

The Embedded OS Team in the Operating Systems and Embedded Technology Division and the Enterprise Application Division at NSA concluded that the Boeing SNS passes the AVA_VLA.3 and AVA_CCA.2 requirements outlined in the Security Target at EAL 5. This determination was based upon a lengthy investigation and thorough analysis of evidence. The results of the formal modeling and verification (including assumptions), SNS source code, and SNS documentation greatly assisted the analysis and testing. As a result, the evaluation successfully searched many details of the Boeing SNS for weaknesses and vulnerabilities. This effort revealed no exploitable vulnerabilities in the Boeing SNS.

The Validation Team, therefore, concludes that the Pass result for the Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) EAL 5 evaluation is complete and correct.

# 11 Annexes

Not applicable.

# 12 National and International Interpretations and Precedent Decisions

The evaluation team performed an analysis of the international interpretations and identified that none are applicable to the Boeing SNS evaluation.

Neither the Security Target nor the vendor's evidence identified any national interpretations. As a result, since national interpretations are optional, the evaluation team did not consider any national interpretations as part of its evaluation. Likewise, the evaluation team did not consider anything from the precedent database.

# 13 Security Target

The Security Target is identified as *Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) Security Target, Version 2.5, 2/3/2011*.

# 14 Glossary

The following definitions are used throughout this document:

- **Attribute.** A characteristic or trait of an entity that describes the entity; for example, the telephone number of an employee is one of that employee's attributes. An attribute may have a type, which indicates the range of information given by the attribute, and a value, which is within that range.
- **Audit Trail.** Data, in the form of a logical path that links a sequence of events, used for tracing the transactions that affected the contents of a record.
- **Authentication.** Verification of the identity of a user or the user's eligibility to access an object.
- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
-

# 15 Bibliography

The Validation Team used the following documents to produce this Validation Report:


[1] Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) Security Target, Version 2.5, 2/3/11.

[2] Common Criteria for Information Technology Security Evaluation (CC), Version 2.3, August 2005 (aligned with ISO/IEC 15408).

[3] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[4] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 2005, version 2.3

[5] Evaluation Technical Report for Boeing Secure Network Server (SNS-3010, SNS-3110, and SNS-3210) EAL 5 Evaluation Part II version 1.0, February 6, 2007.

[6] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.