National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Common Criteria Evaluation and Validation Scheme
Validation Report

SecureInfo Risk Management System (RMS)
Version 3.2.06.12

Report Number: CCEVS-VR-06-0030

Dated: 26 June 2006

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Dr. Jerome Myers
The Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory
COACT CAFÉ Laboratory
Columbia, Maryland 21046-2587

Table of Contents

1 EXECUTIVE SUMMARY 5

2 Identification 5

2.1 Applicable Interpretations 6

3 Security Policy 7

3.1 Access Control Policy 7

3.2 User Authentication 7

3.3 Roles 7

3.4 TOE Separation 7

3.5 Security Function Strength of Function Claim 7

3.6 Protection Profile Claim 8

4 Assumptions 8

4.1 Physical Assumptions 8

4.2 IT Environment Assumptions 8

4.3 Threats 8

4.3.1 Threats Addressed by the TOE 8

4.3.2 Threats Addressed by the Operating Environment 9

5 Clarification of Scope 9

6 Architecture Information 9

6.1 Evaluated Configuration 10

7 Product Delivery 11

8 IT Product Testing 12

8.1 Evaluator Functional Test Environment 12

8.2 Functional Test Results 14

8.3 Evaluator Independent Testing 14

8.4 Evaluator Penetration Tests 15

8.5 Test Results 16

9 RESULTS OF THE EVALUATION 16

10. VALIDATOR COMMENTS 16

11. Security Target 17

12. List of Acronyms 17

13. Bibliography 17

List of Figures

Figure 1: RMS TOE Boundary within Server PC 10
Figure 2: Test Bed Configuration 14

List of Tables

Table 1: Evaluation Identifier 6
Table 2 :Client Hardware/Software Requirements 11
Table 3: Database Server Hardware/Software Requirements 11
Table 4: Functional Test Configuration 12

1 EXECUTIVE SUMMARY

This report documents the NIAP Validators' assessment of the CCEVS evaluation of the SecureInfo RMS Version 3.2.06.12 at EAL2. It presents the evaluation results, their justifications, and the conformance result.

The evaluation was performed by the CAFE Laboratory of COACT Incorporated, located in Columbia, Maryland. The evaluation was completed on 26 June 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) written by COACT and submitted to the Validators. The evaluation determined the product conforms to the CC Version 2.2, Part 2 and Part 3 to meet the requirements of Evaluation Assurance Level (EAL) 2 resulting in a "pass" in accordance with CC Part 1 paragraph 175.

The TOE is the application software that resides on a web server. The SecureInfo RMS product is a software tool that is marketed to support Certification and Accreditation (C&A) activities. The TOE generates security Certification and Accreditation (C&A) document templates that a customer can tailor for compliance with government and other regulatory mandates. Due to the potential sensitivity of the information contained in the documents managed by RMS, RMS provides mechanisms to limit accessibility to those with a need-to-know. Therefore, RMS supports identification and authentication, access control, and role management features. These features limit access to RMS, RMS data elements, and support three roles: RMS system administrator, domain manager, and user. These security features were the focus of the CC evaluation. In addition to the RMS application, the server consists of the underlying hardware, operating system, Apache Tomcat Web Server, MS SQL Server, and Java Runtime Environment. Those components of the server were not included in the evaluation. Moreover vendor claims regarding suitability of RMS for use in C&A activities were not covered by this evaluation.

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 Evaluation Assurance Level (EAL) 1 through EAL 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 desire 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 CCEVS' 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 organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifier

Evaluation Identifiers for SecureInfo RMS 3.2.06.12	
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	SecureInfo Risk Management System Version 3.2.06.12
Protection Profile	N/A
Security Target	SecureInfo Risk Management System 3.2.06.12 Security Target, Version 1.0 dated June 26, 2006
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation SecureInfo RMS 3.2.06.12 ETR, Document No. F2-0606-003, Dated June 26, 2006
Conformance Result	Part 2 conformant and EAL2 Part 3 conformant
Version of CC	CC Version 2.2 [1], [2], [3], [4] and all applicable NIAP and International Interpretations effective on February 2, 2005
Version of CEM	CEM Version 2.2 and all applicable NIAP and International Interpretations effective on February 2, 2005
Sponsor	SecureInfo 211 North Loop 1604 East Suite 200 San Antonio, TX 78232
Developer	SecureInfo 211 North Loop 1604 East Suite 200 San Antonio, TX 78232
Evaluator(s)	**COACT Incorporated** Brian Pleffner Christa Lanzisera Anthony Busciglio
Validator(s)	**NIAP CCEVS** Dr. Jerome Myers

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

I-0418 – Evaluation of the TOE Summary Specification: Part 1 Vs Part 3
I-0426 – Content of PP Claims Rationale
I-0427 – Identification of Standards

International Interpretations

None

3 Security Policy

The TOE is a software tool executing on a dedicated server. The TOE is accessed from client workstations through a network interface to the server. The TOE controls access to a specific set of documents and templates that are intended to be used in the development of Certification and Accreditation evidence. The security features of the TOE limit access to RMS, RMS data elements, and support three roles: RMS system administrator, domain manager, and user.

3.1 Access Control Policy

The TOE enforces an access control policy that restricts the operations that users can perform on the RMS controlled data elements. There are 18 distinct types of operations that can be performed on 26 distinct types of objects. Section 5.3.1 in the Security Target states which specific operations are possible on each of the types of objects. The access control policy permits the restriction of those possible operations to users based upon individual identities or by grouping of the individual users into sets called “domains”. The TOE uses access control to address security attribute usage and characteristics of policies and may have the ability to explicitly authorize or deny access to an object based upon security attributes. Specifically, security attribute-based access control allows the TOE to enforce access and operations based upon security attributes and named groups of attributes.

3.2 User Authentication

The TOE requires users to identify and authenticate themselves before accessing the TOE and, therefore, by default, before viewing any TSF data or configuring any portion of the TOE. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that defines the functionality the user is allowed to perform.

3.3 Roles

The TOE defines and enforces three types of security roles: *Authorized RMS System Administrators*, *Domain Managers*, and *Authorized Users.* These roles are managed within the TOE. An Authorized RMS System Administrator has the ability to define groups and other roles to assist in the management of access rights and privileges. A Domain Manager has full access to and has the ability to create user accounts in his or her domain. Authorized Users are users that are authorized to use some TOE resources.

3.4 TOE Separation

The TOE ensures that all functions are invoked and succeed before the next function may proceed.

3.5 Security Function Strength of Function Claim

The only mechanism in the TOE for which an SOF claim is required is the Password mechanisms for user authentication which is SOF-basic.

3.6 Protection Profile Claim
This Security Target does not claim conformance to any registered Protection Profile.

4 Assumptions

The specific conditions listed in the following subsections are assumed to be met by the environment and operating conditions of the system. The assumptions are ordered into three groups. They are personnel assumptions, physical assumptions, and IT environment assumptions.

A) Personnel assumptions describe characteristics of personnel who are relevant to the system.

B) Physical environment assumptions describe characteristics of the non-IT environment that the system is deployed in.

C) IT environment assumptions describe the technology environment within which the TOE is operating.

4.1 Physical Assumptions
The results of the evaluation rely upon the assumption that the processing resources of the TOE will be located within controlled access facilities that will prevent unauthorized physical access.

4.2 IT Environment Assumptions
The results of the evaluation rely upon the following assumptions regarding the IT Environment.

AE.CONNECT	Any other systems with which the TOE directly and interactively communicates is under the management control of the organization in which the system is deployed and operates under the same security policy constraints as the TOE.
AE.PROTECT	The hardware and software critical to the execution of the TOE will be protected from unauthorized access.
AE.JUSTAPPS	Applications executing on the RMS server are limited to the TOE and applications that the TOE is dependent on for proper and secure execution. No other application will be installed, generated, or executed on the RMS server.

4.3 Threats
The following threats are addressed by the TOE and IT environment, respectively.

4.3.1 Threats Addressed by the TOE

The TOE addresses the following threats:

T.ACCESS	An unauthorized individual may attempt to gain access to the TOE, a TOE resource, or to information directly controlled by the TOE, via user error, system error, or an unsophisticated, technical attack.
T.NOAUTH	An authorized user may attempt to access information specific to the RMS System Administrator, Domain Manager or another user that is stored by the TOE by circumventing the access control function.

4.3.2 Threats Addressed by the Operating Environment

The TOE relies upon the IT Environment to protect the server platform on which the TOE resides. The associated threat that is addressed by the IT Environment Requirements is:

TE.ACCESS	An unauthorized individual may gain access to information not protected by the TOE in the operating environment, including TOE data stored outside the TOE.

5 Clarification of Scope

The evaluation of SecureInfo RMS covers the documentation access controls and associated administrative roles that are implemented by RMS. The evaluation does not make any statements about the adequacy or effectiveness of the RMS product for its advertised usage in the development and maintenance of Certification and Accreditation documentation.

General user access to the TOE is through a network interface. The vendor provides a client application that executes on workstations and provides a GUI interface to the TOE. The client application and associated network communications protections (based upon SSL) were not part of this evaluation. This evaluation only covered the RMS server application.

In addition to the RMS application, the server consists of the underlying hardware, operating system, Apache Tomcat Web Server, MS SQL Server, and Java Runtime Environment. The evaluated TOE relies upon those other components of the server to protect the TOE and restrict access to the server platform to users that must access the server through the TOE provided network interface. Those other components of the server are included in the IT Environment and hence not covered by this evaluation.

6 Architecture Information

The TOE consists of a software application running on a dedicated server. Access to the TOE is performed over the network using the network server interface. The vendor provides client software that executes on workstations. Although those clients were used for portions of the TOE evaluation, the client applications are not part of the evaluated TOE. The evaluated TOE resides entirely within the server. Figure 1: RMS TOE Boundary within Server PC illustrates the server configuration and the associated TOE boundary.

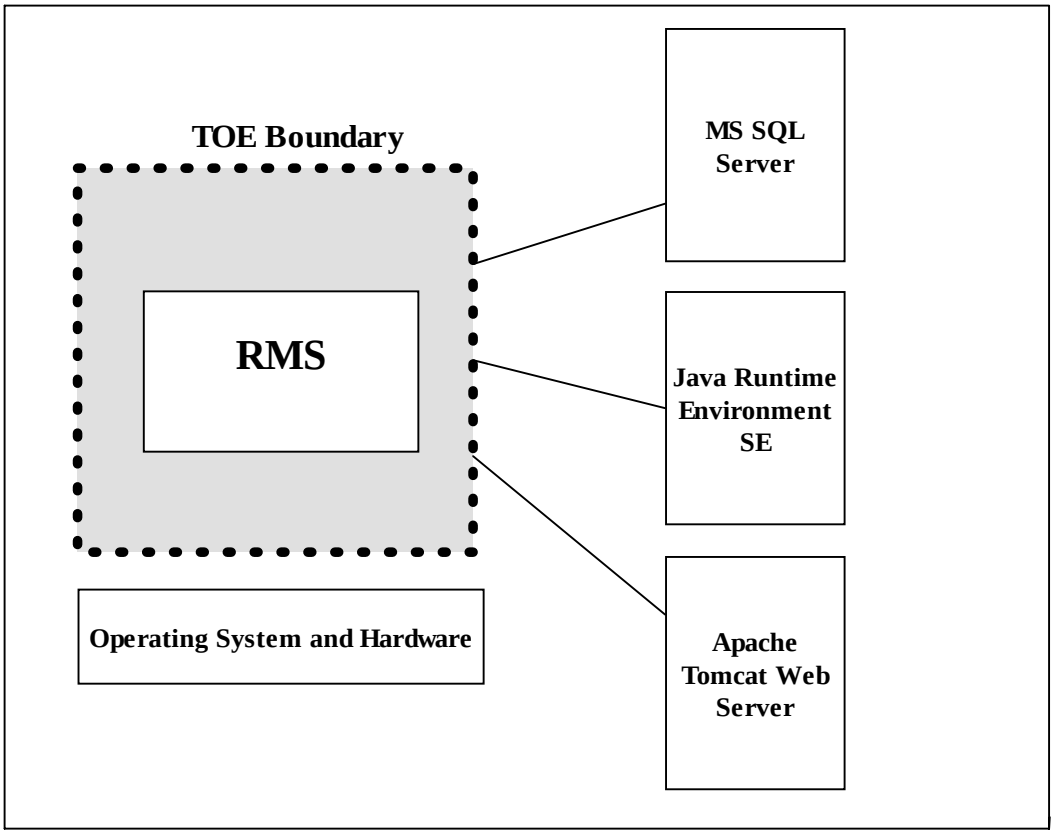

Figure 1: RMS TOE Boundary within Server PC

6.1 Evaluated Configuration

The evaluated configuration of the TOE is depicted in Figure 1: RMS TOE Boundary within Server PC above. The parameters of the TOE that are outside the scope of evaluation are the underlying operating system and associated hardware, MS SQL Server 2000, Java Runtime Environment SE and Apache Tomcat Web Server. The Operational Environment is addressed in Table 1 and 2 below. In addition, the entire Client (hardware/software) used to access the TOE is outside the scope of this evaluation.

The following tables specify the hardware and software required for the operation of the TOE. Table 2 specifies client information that is not part of the evaluated TOE and Table 3 specifies the hardware and software that is required to be configured on the server platform for the evaluated TOE.

Table 2: Client Hardware/Software Requirements

Hardware	Software
Intel platform or compatible Intel Pentium 3 800 MHz or higher 256 MB RAM 1 GB Hard Drive Network connection	MS Windows 2000 (all editions) MS Internet Explorer 6.0 or higher

Table 3: Database Server Hardware/Software Requirements

Hardware	Software
Intel platform or compatible Intel Pentium 4 2.0 GHz or higher 1 GB RAM 40 GB Hard Drive Network connection	MS Windows 2000 Server or Windows 2003 Server with current Service Packs and Hot fixes MS Internet Explorer 6.0 or higher Sun Java 2 SE SDK 1.4.2_04 MS SQL Server 2000 SP3a Apache Tomcat 4.1.30 MS SQL Server 2000 Driver for JDBC SP2, The driver must be installed in the <Tomcat base>\ common\ lib folder.

7 Product Delivery

The TOE delivery includes two CDs and some hard copy documentation. One CD is labeled as the "RMS Application Content CD" and the other CD is labeled as the "RMS Documentation CD". The two CDs are delivered in a double CD case with two paper inserts. The inserts are titled:

1) Configuration Manager Quick Start Guide; and
2) User Quick Start Guide

These two inserts were included in the evaluated documentation for the TOE.

The RMS Application Content CD contains the following items:

1) SecureInfo RMS Server Application Version 3.2.06.12
2) Sun Java SDK 1.4.2_06 (Server)
3) Apache Tomcat 4.1.30
4) Sun Java Runtime Environment SE 1.4.2_06 (Client)

The first item is the software application that was included in the evaluation. The other three Items are installed as part of the IT Environment. Items 2 and 3 must be installed on the server host and Item 4 must be installed on the client to enable client access to the TOE.

The RMS Documentation CD contains soft copies of the following items that were part of the evaluation:

1) RMS 3.2.06 Content Administration Guide
2) RMS 3.2.06 Enterprise Administration Guide, dated 2006
3) RMS 3.2.06 Installation Guide, Dated 2006

All of the documents present on the Documentation CD were covered by the evaluation.

A “Marketing Collateral” folder with Customer Support business card and a “Welcome” letter are also delivered with the TOE. Neither of those two items were included in the scope of the evaluation.

8 IT Product Testing

Testing was performed on May 25 and May26 2006 at the COACT Laboratory in Columbia, MD. Two COACT employees performed the tests. The Lead Validator and two other validation observers were present for portions of the testing, but they did not observe all of the testing. During some pretest activities earlier that month the CCTL identified a TOE vulnerability that needed to be fixed. The vendor made the appropriate changes to the TOE, but was unable to deliver the updated product through the evaluated delivery mechanism in time to start the testing. As a result, the evaluators used an electronic download procedure to obtain the TOE that was installed for testing. After that testing activity, an official delivery of the TOE was received and a digital comparison was performed to ensure that the tested version of the TOE was in fact the evaluated version of the TOE.

8.1 Evaluator Functional Test Environment

Testing was performed on a test configuration consisting of three PCs connected through a Hub. Only two of the PCs were used for functional testing. The third PC shown in the test configuration was not used for functional testing, but was used for penetration testing. One PC was configured as a Server for the TOE and a second PC was configured as a Client for the TOE. Figure 2: Test Bed Configuration on page10 shows the topology of the test bed configuration. The hardware and software configurations for the server and client for functional testing is detailed below in Table 4

Table 4: Functional Test Configuration

System	Hardware Minimum Required	CCTL Test Platform Hardware	Minimum Software Requirements	CCTL Test Platform Software
Server	Intel Platform or Compatible Intel Xeon Processor 2.0 GHz or higher 1 GB RAM 40 GB Hard Drive Network Connection	3.2 GHz Pentium IV 2 GB RAM 80 GB Hard Drive Network Connection	MS Windows 2000 Server or Windows 2003 Server with current Service Packs and Hotfixes MS Internet Explorer 6.0 or higher Sun Java 2 SE SDK 1.4.2_06 (Included on the RMS 3.2.06.12 CD) MS SQL Server 2000 SP3a Apache Tomcat 4.1.30 (Included on	MS Windows 2000 Server MS Internet Explorer 6.0 Sun Java 2 SE SDK 1.4.2_06 (Included on the RMS 3.2.06.12 CD) MS SQL Server 2000 SP3a Apache Tomcat 4.1.30 (Included on the RMS 3.2.06.12 CD)

			the RMS 3.2.06.12 CD) MS SQL Server 2000 Driver for JDBC SP3 The driver must be installed in the <Tomcat base>\ common\ lib folder	MS SQL Server 2000 Driver for JDBC SP3
Client	Intel Platform or Compatible Intel Pentium III 800 MHz or higher 256 MB RAM 1 GB Hard Drive Network connection		MS Windows 2000 (all editions) MS Internet Explorer 6.0 or higher Sun Java Runtime Environment SE 1.4.2_06 (Included on the RMS 3.2.06.12 CD) MS Excel or the MS Excel Viewer (all versions)	

The table shows both the minimum required hardware/software configuration to operate the RMS 3.2.06.12 software in the TOE configuration and the actual hardware/software configuration the CCTL used to conduct the vendor tests and independent tests. Appropriate analysis was performed and evidence presented to ensure that the results from testing on this test configuration applied to all variant configurations of the evaluated TOE.

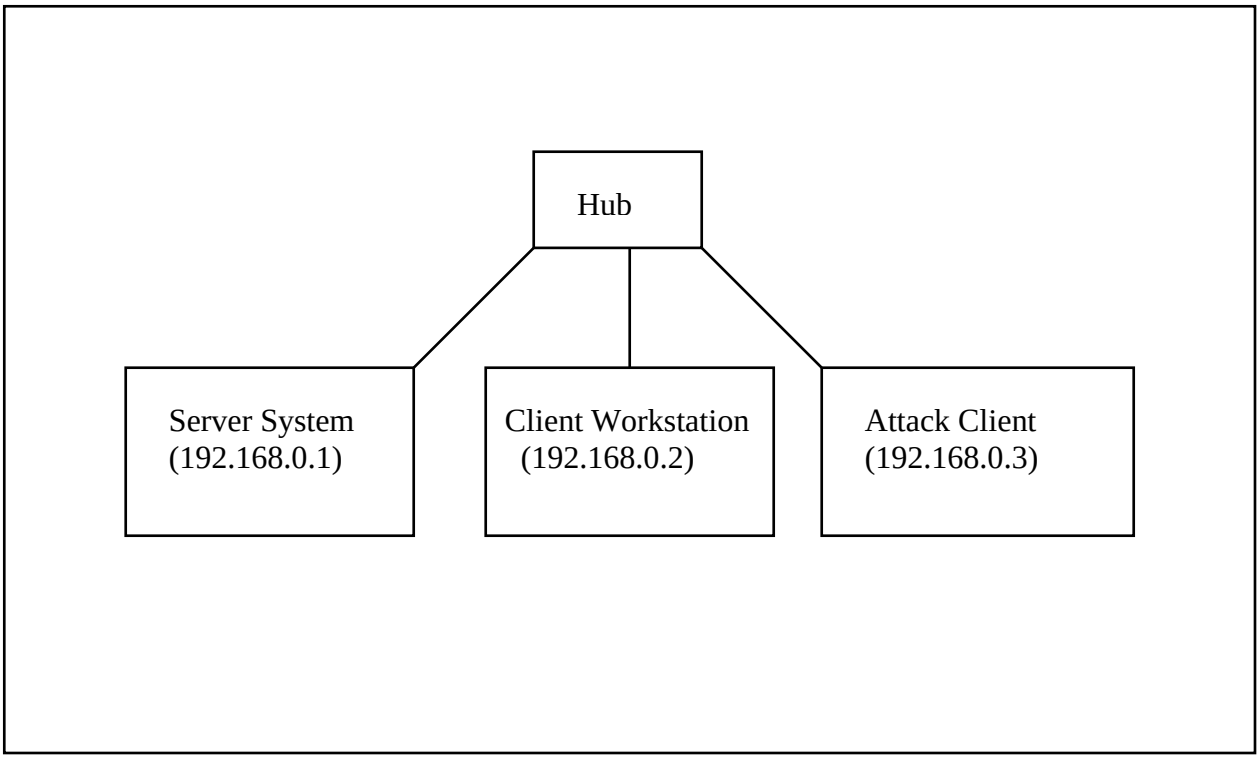

Figure 2: Test Bed Configuration

8.2 Functional Test Results

The evaluation team executed the entire developer test suite. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests. The procedures followed to execute these tests and detailed results are presented in the developer and CCTL proprietary report, *Secure Info RMS 3.2.06.12 Functional Test Report, dated June 26, 2006*.

8.3 Evaluator Independent Testing

The evaluation team performed an analysis of all of the developer tests to assess the level of developer testing corresponding to each of the TSFIs. As a result, they identified five TSFIs that were not fully covered by the developer testing. The evaluators performed independent testing for each of those interfaces. The following tests were performed during independent functional testing:

1) Ensure that a User can be created both disabled and enabled and attempt to log in with that user while both enabled and disabled
2) Attempt RMS Administrator deletion of a domain, attempt a Domain Administrator deletion of his own domain and another domain
3) Attempt RMS Administrator modification of a domain's password rules, attempt a Domain Administrator modification of his own domain's password rules and another domain's password rules
4) Attempt RMS Administrator removing permission for a user, attempt a Domain Administrator removing permission for a user in his own domain and another domain
5) Open various object with the system and log off. Then log in as another user and ensure access to those objects.

The test environment used for the evaluation team's independent tests was identical with the test configuration used to execute the vendor tests. All tests were performed satisfactorily and the results were as expected. The TOE passed all tests.

8.4 Evaluator Penetration Tests

The evaluators examined each of the obvious vulnerabilities identified during the developer's vulnerability analysis. While verifying the information found in the developer's vulnerability assessment, the evaluators conducted a search to verify that no additional obvious vulnerabilities existed for the TOE.

After verifying that the developer's analysis approach sufficiently included all of the necessary available information regarding the identified vulnerabilities, the evaluators made an assessment of the rationales provided by the developer indicating that the vulnerability was non-exploitable in the intended environment of the TOE. Any possible vulnerability that required further evaluator analysis was identified as "suspect". The evaluators identified six "suspect" potential vulnerabilities that warranted further analysis. However, after performing a threat analysis on each of those vulnerabilities, the evaluators reached the same conclusion as was in the vendor analysis; i.e. further testing of those vulnerabilities was unnecessary.

While verifying the information found in the developer's vulnerability assessment the evaluators conducted a search to verify if additional obvious vulnerabilities exist for the TOE. Additionally, the evaluator examined the provided design documentation and procedures to attempt to identify any additional vulnerabilities.

As a result of the evaluator's examination of the developer's vulnerability analysis and the independent search for obvious TOE vulnerabilities, the evaluator devised a test plan and a set of test procedures to test the TOE's mitigation of the vulnerabilities. The scope of evaluator analysis and testing included potential obvious vulnerabilities in the IT Environment that would be introduced as a result of the presence of the TOE. The following Penetration tests were performed by the evaluator:

- #1 Port scans to confirm that all ports that could facilitate insecure management to/communication with the TOE are not available.
- #2 Attempt to compromise the HTTPS stream between the client and server to retrieve TSF data.
- #3 Running of Tiger Test Suite to verify that the TOE is not susceptible to readily available application vulnerability exploits.
- #4 Sniffing client/server communication to verify secure communication.
- #5 While a user is logged in, having an administrator modify the permissions of the user and observing the TOE response.

The test configuration is illustrated in Figure 2. It consisted of a network (represented by three PCs connected through a hub), the SecureInfo RMS 3.2.06.12 Server installed on one of the PCs, the RMS 3.2.06.12 Agent and Console on two other PCs: one used to act to support an authorized user and the other used to act as an attack client. The server and the client workstation were configured as for functional testing. The configuration of those hosts is provided in Table 4: Functional Test Configuration. The "Attack Client" was also configured with the software and hardware specified for a client in Table 4, but in addition to the TOE software the following four software applications were installed on the attack client.

A) NeWT, version 2.2.1

B) NMap, version 0.2
C) Ethereal, version 0.10.11
D) ParosProxy, version 3.2.11

The results of the testing activities were that all tests gave expected (correct) results. No vulnerabilities were found to be present in the evaluated TOE. The results of the penetration testing are documented in the vendor and CCTL proprietary report, COACT document F2-0606-001(1) *Secure Info RMS 3.2.06.12 Penetration Test Report, dated 26 June 2006*.

8.5 Test Results

The end result of the testing activities was that all tests gave expected (correct) results. The successful completion of the evaluator penetration tests demonstrated that the TOE was properly resistant to all the potential vulnerabilities identified by the evaluator. The testing found that the product was implemented as described in the functional specification and did not uncover any undocumented interfaces or other security vulnerabilities in the final evaluated version. The evaluation team tests and vulnerability tests substantiated the security functional requirements in the ST.

9 RESULTS OF THE EVALUATION

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence.

In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Section 4, Results of Evaluation, from the document *Evaluation Technical Report for the Secure Info Risk Management System (RMS) Version 2.0.6.12, dated June 26, 2006* contains the verdicts of “PASS” for all the work units.

The evaluation determined that the product meets the requirements for EAL 2. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by COACT Inc.

10. VALIDATOR COMMENTS

During the course of the evaluation, the evaluation team identified and had the vendor fix a potential vulnerability of the TOE that was demonstrated to be present in the proposed TOE. The validator was pleased with the efficient and cooperative manner in which the matter was handled by both the CCTL and the TOE developers.

All other validator comments are already captured in the Clarification of Scope section (page 9) of this report.

11. Security Target

The Security Target document, *SecureInfo Risk Management System (RMS) Version 3.2.06.12 Security Target, Version 1.0, June 26, 2006* is incorporated here by reference.

12. List of Acronyms

CC	Common Criteria
CCEVS	Common Criteria Evaluation Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
C&A	Certification and Accreditation
EAL	Evaluation Assurance Level
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute for Standards Technology
PP	Protection Profile
RMS	Risk Management System
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

13. Bibliography

The following list of standards was used in this evaluation:

- Common Criteria for Information Technology Security Evaluation, Part 1 Introduction and General Model, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 2 Security Functional Requirements, Version 2.2, dated January 2004
- Common Criteria for Information Technology Security Evaluation, Part 3 Security Assurance Requirements, Version 2.2, dated January 2004

- Common Methodology for Information Technology Security Evaluation, Part 1, Version 2.2, dated January 2004
- Common Methodology for Information Technology Security Evaluation, Part 2, Version 2.2, dated January 2004
- Guide for the Production of PPs and STs, Version 0.9, dated January 2000