DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

CMS Reporting Standard for Information Security Testing

Version # 4
July 15, 2005

SUMMARY OF CHANGES

V4.0

1. Changed references to the CMS Application Testing Approach document to the CMS Information Security Testing Approach to reflect the change in the title of the document.

2. Clarified the narrative use of "Business Risks" and "Findings" within the Exectuive Summary, section 2, of the Report Template.

3. Detailed description of the following sub-sections inserted into the second paragraph of Detailed Findings, section 3, of the Report Template.

4. Defined "Procedural Vulnerabilities" in Procedural Business Risks (If Any Were Identified), section 3.3, of the Report Template.

5. Defined "Technical Vulnerabilities" in Technical Business Risks (If Any Were Identified), section 3.4, of the Report Template.

6. Added narrative to Section 4, Guidelines for Documenting Business Risk, to reflect the changes throughout the document and revisions to the CMS IS Business RA Methodology and the IS RA Methodology.

7. Reduced section 5.4, Report Package Documentation, sub-sections to reflect the changes to the POA&M instructions and form(s).

8. Added a boiler-plate narrative to section 3, Detailed Findings, of the Report Template that addresses observations defined as "vunlerabilities beyond the scope of the test".

9. Added narrative to "How to Use This Template" within Appendix A.

10. Eliminated Appendix B, Business Risk Template, due to redundant templates within the Procedural Business Risks section and Technical Business Risks section.

11. Replaced Appendix C, Findings Tracking Template, Appendix D, Weakness Summary Report Template, and Appendix E, POA&M Form, with a single appendix called, Appendix B - POA&M Instructions and Tracking Form which now includes original the POA&M Form from the old Appendix E.

12. Added the Instructions for POA&M Tracking Form to the new appendix, "POA&M Instructions and Tracking Form."

13. Updated the Test Scripts format to reflect the latest versions, minor grammar correction and included examples to demonstrate what type of data should be used.

14. Added new Appendix C - Test Plan Templates that include YR1 ST&E Test Plan Template and YR2 ST&E Test Plan Template.

15. Renamed Test Plan Template to YR1 ST&E Test Plan Template.

16. Added new Appendix D – Test Script Template.

V3.0

1. Section 3.6 Security Test Report Package includes the additional information reflecting the working papers documentation and the differing versions of the packages for CMS, system owners and other responsible entities.

2. Section 5.4 Original Working Papers Section requirement added, containing the following parts / requirements:
   - Test Plan;
   - Test Script;
   - Communications;
   - Supporting Papers; and
   - Working Papers.
3. Section 5.5 CD-ROM requirement added.
4. Section 5.3 Weakness Tracking Form changed to 5.3 POA&M Form.
5. Appendix C POA&M Template changed to Appendix C Findings Tracking Template.
6. Appendix E Weakness Tracking Template changed to Appendix E POA&M Template.
7. Appendix F Test Plan Template added as supplemental guidance to Section 5.4.1.
8. Appendix G Test Script Template added as supplemental guidance to Section 5.4.2.
9. Added Section 3.4.1 CMS Findings Numbering Standards.
10. Section 3.4.1 through 3.4.3 moved to 3.4.2 through 3..4.4, due to addition of Section 3.4.1 CMS Findings Numbering Standards.

V2.0

Formatting changes only

TABLE OF CONTENTS

SUMMARY OF CHANGES I
TABLE OF CONTENTS III
1. INTRODUCTION 1
1.1 Statement of Purpose 1
1.2 Core Requirements and Considerations 1
1.3 Goals and Objectives 2
2. APPROACH 3
3. REPORT STRUCTURE 4
3.1 Introduction 4
3.2 Scope 4
3.3 Executive Summary 5
3.4 Detailed Findings 5
3.4.1 CMS Findings Numbering Standards 5
3.4.2 Methodology of Vulnerability Testing 8
3.4.3 Methodology of Security Test Reporting 8
3.4.4 Business Risks 9
3.5 Report Appendices and Attachments 9
3.6 Security Test Report Package 9
4. GUIDELINES FOR DOCUMENTING BUSINESS RISKS 10
4.1 Guidelines for Assessing Risk Level 10
4.2 Guidelines for Assessing Ease-of-Fix 12
4.3 Guidelines for Assessing Estimated Work Effort 13
4.4 Security Control Families 14
4.5 Common Vulnerability and ExPosure Numbers 19
4.6 Business Risk Description 19
4.7 Suggested Corrective Action 20
4.8 Status 20
5. REPORT PACKAGE DOCUMENTATION 21
5.1 POA&M Tracking Form 21
5.2 ORIGINAL WORKING PAPERS SECTION 21
5.2.1 Test Plan 22
5.2.2 Test Script 22
5.2.3 Communications 22
5.2.4 Supporting Papers 23
5.2.5 Working Papers 23
5.3 CD-ROM 23

APPENDIX A – SECURITY TEST REPORT TEMPLATE.....25
APPENDIX B – POA&M INSTRUCTIONS AND TRACKING FORM.....41
APPENDIX C –TEST PLAN TEMPLATES.....44
C.1 YR1 ST&E TEST PLAN TEMPLATE.....45
C.2 YR2 ST&E TEST PLAN TEMPLATE.....60
APPENDIX D –TEST SCRIPT TEMPLATE.....75

1. INTRODUCTION

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health & Human Services has tasked JANUS Associates, Inc. (JANUS) to develop a reporting standard for information security testing. The information types to be included within security test reports are defined by, or consistent with, National Institute of Standards and Technology (NIST), Federal Information System Controls Audit Manual (FISCAM), and CMS Information Security (IS) policy and standards requirements, and the security test report template has been designed to include information sufficient to facilitate risk analysis / risk assessment, and to track vulnerabilities and corrective actions plans (CAP). This document establishes the standard report template, and provides guidance for CMS employees and CMS contractors in documenting and reporting security test results.

1.1 STATEMENT OF PURPOSE

The reporting model is the standard for reporting of security test results, such that:

1. Security test results of technically and administratively unrelated information systems are presented in a consistent format, independent of hardware and software configurations, management processes, or organizational hierarchy;

2. The effectiveness of security controls implemented on technically and administratively unrelated information systems can be evaluated comparatively, with respect to information sensitivity level; and

3. The ability to gauge the effectiveness of security controls, security management processes, and security improvements is enhanced.

1.2 CORE REQUIREMENTS AND CONSIDERATIONS

In completing the CMS business mission, highly sensitive and critical information is processed, stored, and transmitted through a complex infrastructure of CMS-owned and contractor-operated information systems. To support CMS business requirements, use of diverse information technology components and platforms are required. To ensure that the confidentiality, integrity, and availability of information are adequately protected, CMS must implement effective management, operational, and technical security controls that reduce risk to an acceptable level. Security testing is required to evaluate and / or validate the effectiveness of such controls and to identify any vulnerability in the information systems. Security test results shall be documented and formatted in a way that conveys this information to CMS and trusted business partners, if applicable, which can feed internal risk management processes. Security test reports must contain information sufficient for management to render informed, risk-based decisions. To achieve consistent reporting across diverse business functions, information technology platforms, and business units, the reporting model must be independent of the CMS business and technological infrastructures.

The reporting model is designed to represent the security testing results as risks to the business of CMS. To analyze and report the CMS Business Risks properly, it is critical to consider the potential business impact if technical and procedural security threats materialize, as well as the anticipated threat exposure. The business impact depends substantially upon the sensitivity requirements of the information at risk of disclosure or modification. The reporting standard establishes clear guidelines for assessing risk level based upon the potential business impact and threat exposure of each vulnerability. The standard ensures that security testing of all information systems is reported in a comparative fashion, and that security controls for information with corresponding sensitivity levels are consistently measured.

1.3 GOALS AND OBJECTIVES

The principle design goals of CMS are to establish a reporting model which:

1. Is flexible enough to apply to all current and future CMS infrastructures and / or infrastructures supporting CMS information systems; yet,

2. Is specific enough to provide accurate results and comparative measurements for all types of security testing, regardless of systems reviewed.

3. Enables CMS to compare security test results over time, and clearly identifies categorical improvements or deteriorations.

4. Is easy to implement, use, and understand, for a system that favors clearly defined reporting guidelines and results.
    a. The reporting standard should not require undue training and preparation time, should be readily adaptable to the CMS environment, including those of our business partners, and should not substantially increase the work effort of CMS staff or of independent security testers.
    b. The standard should clearly define the processes and responsibilities for security test reporting, with firm guidelines for assessing risk level and remediation effort.

5. Provides a firm level of consistency, such that similar testing results will be reported in a uniform manner, regardless of tester or information system.

6. Defines and utilizes terminology in a consistent fashion.

2. APPROACH

Following completion of an information security test, this document shall be used by CMS staff or CMS contractors to document the security test and / or System Test & Evaluations (ST&E) results. The following sections provide guidance for the production of security test reports. Report authors shall develop a draft report, marked as such, and deliver the draft version to CMS. CMS shall then review the draft report, provide feedback to the report's author, and, if necessary, schedule a meeting to discuss open issues or to clarify findings. The reports' authors must then make any required revisions to the report, and produce a final report, labeled accordingly. The final report shall be delivered to CMS, along with any and all working papers in hard copy or electronic format, which shall include all test results, notes, and screenshots. The report's author shall also prepare and submit an appropriate Plan of Action and Milestones (POA&M) Tracking Form along with the final report.

Appendix A to this document includes the standard CMS security test report template that shall be used to report the security test results. The report template includes a section that independently addressees each vulnerability discovered during the testing process, and details the Business Risk to CMS. The standard report format will enable CMS to review the results of security testing performed on unrelated technical systems in a common method. The standard format ensures that all testing results are subject to identical assessment guidelines, and reports include the same types of information. Section 3 describes the report format, and defines requirements for the production and delivery of the Security Test Report Package.

In any security test, an adequate level of discretion in reporting results must be afforded to the tester. This provides the flexibility to address the test results truly from a business or "real-world" perspective, and permits expansion of reporting applicability. In order to achieve standardization, however, the discretion granted to individual testers must be limited in order to prevent excessive bias and subjectivity from entering the report. The assessment guidelines (Section 4) are intended to limit the levels of personal and organizational discretion in order to prevent reporting inconsistencies, yet permit an acceptable level of discretion and provide adequate flexibility.

A key component of security test reporting is the assessment of risk level and remediation effort for each vulnerability. The CMS reporting model includes an assessment of the risk level for each vulnerability, the ease of mitigating or repairing each vulnerability, and the estimated work effort required to implement reasonable and appropriate controls. The analysis is based upon guidelines that facilitate the assessment of each risk or fix level. When evaluating the level of risk, the ease of remediation, and the estimated work effort associated with correcting or controlling the exposure, a qualitative approach based upon structured guidelines is the appropriate method.

To facilitate CMS in evaluating, monitoring, and comparing the effectiveness of security controls across diverse operating environments and platforms, each Business Risk shall be associated with at least one security control family. Grouping of Business Risks into security control families will enable CMS to identify categorical weaknesses common to similar or dissimilar information systems, and dedicate resources to those control families that, if strengthened, will

reduce or close the greatest number of vulnerabilities. Currently the seventeen (17) security control families described in NIST Special Publication 800-53 shall be used for this purpose.

3. REPORT STRUCTURE

The purpose of a security test report shall be to communicate the test results at the level of the intended audience. In nearly all situations, security test results are provided to several audience levels, ranging from Senior Management to technical staff. Senior Management (or any high-level reader) is not interested in the technical details of a given vulnerability, but rather the "big picture". It is crucial that a security test report enables high-level audiences to understand, quickly and proficiently, the potential impact of security vulnerabilities, and what those results mean to the business. This enables management to render informed decisions regarding security expenditures and staffing. On the other hand, technical personnel must fully understand the details of a given vulnerability in order to plan successfully for and take appropriate corrective action. For this reason, it is necessary to provide full details of all vulnerabilities discovered through security testing.

To accommodate the competing needs of potential audiences, the report format shall provide an initial discussion of the "big picture", followed by technical details at a lower level. The "Executive Summary" section in the beginning of the report presents a high-level overview of the security test results, without the need for non-technical readers to examine the entire report. The next section includes the detailed Business Risks identified through testing, which describe the technical details of each vulnerability discovered. This section enables technical staff to understand fully how the vulnerability was discovered, how it could be exploited, and what corrective actions are necessary to close or reduce the impact of the vulnerability.

The following sections identify and describe the components of the security test report format. Refer to Appendix A for the report template that shall be used to document actual security test results.

3.1 INTRODUCTION

The introduction to the report shall contain a brief description of the security test engagement. The introduction shall: (1) Identify the contractor or CMS personnel who conducted the test; (2) Identify the system or application that was the subject matter of the test; (3) Include the period of performance; and (4) Provide a brief description of the purpose of the assessment. Refer to the report template in Appendix A, which includes sample language for the "Introduction" section.

3.2 SCOPE

The scope of the security testing engagement shall be detailed within the Scope section of the report template. The scope statement shall identify the information system(s) that was tested, including the operating system version, IP address, and any COTS software, and shall define the logical and / or organizational boundaries of the test. Logical boundaries may include network perimeter points or system / network architecture layers. Organizational boundaries may include points of separation between business functions or hosting providers.

3.3 EXECUTIVE SUMMARY

The Executive Summary shall provide a high-level narrative description of the major Business Risks identified during the vulnerability assessment. The primary audience for the Executive Summary is CMS management. The Executive Summary shall: (1) Provide a description of the business function supported by the system or application that was tested; (2) Provide a brief statement of scope for the testing engagement; (3) Briefly summarize the significant vulnerabilities identified during the test; (4) Explain the potential impact of these vulnerabilities; (5) Describe any trends or categorical weaknesses; and (6) Recommend, at a high-level, strategic options or corrective actions necessary to close or reduce the impact of each type of vulnerability. The Executive Summary shall not include any technical details; this information shall be contained within the individual Business Risks.

A maximum of two visual graphs may be included within the Executive Summary, where appropriate. One graph option shall display the distribution of Business Risks between High Risk, Medium Risk, and Low Risk. The second graph option shall display a breakdown of the weaknesses identified per security control family. The appropriateness of including graphs within the Executive Summary depends primarily upon a determination of whether the visual tools are likely to provide added value to the report, such that CMS management will be provided meaningful information that will help to conceptualize and appreciate the significance of the test results.

3.4 DETAILED FINDINGS

The "Detailed Findings" section shall include all individual Business Risks identified during the security test. Prior to the Business Risks, this section shall describe how the test was conducted, what tools and procedures were employed, and how the Business Risks have been analyzed and documented.

3.4.1 CMS FINDINGS NUMBERING STANDARDS

The standards used to identify and enumerate the findings within a report are subject to federal mandates and guidance, as listed in part, in the *Office of Financial Management (OFM) Medicare Financial* Manual, Chapter 7.

In addition to the format of the report following a strict template, as provided within Appendix A, each finding within the report will be numbered in a specific manner to easily identify the contractor, the year of the test, and the type of test / review. This numbering standard will allow CMS to track findings, utilizing various tools without the risk of duplication or the loss of tracked findings.

Findings Numbering Process
The CMS Finding Numbers should be assigned using the following instructions. Each section of digits should be separated by a dash.

- The first three or four digits are letters, which identify the name of the contractor, system or entity responsible for the system. Each contractor / system / entity is assigned a unique set of letters listed in the *OFM Medicare Financial Manual*, Chapter 7.
    - Acronyms will be assigned and utilized within the numbering scheme to designate the contractor / system / responsible entity subject to the review, or the organization responsible for the tested system. The following table lists the contractors / system / entities and their CMS assigned acronyms for the purpose of tracking findings.

Entity Finding Identifiers (from *OFM Financial Manual*)

Contractor / System / Entity	Acronym
AdminaStar Federal Inc.	ASF
Anthem Health Plans of New Hampshire, Inc. (d.b.a. Anthem Blue Cross and Blue Shield of New Hampshire)	ANT
Arkansas Blue Cross and Blue Shield	ARK
Anthem Health Plan of Maine (d.b.a. Associated Hospital Service of Maine)	AHS
Blue Cross and Blue Shield of Alabama (Cahaba Government Benefit Administrators)	ALA
Blue Cross and Blue Shield of Arizona, Inc.	ARZ
Blue Cross and Blue Shield of Georgia, Inc.	GEO
IBM	IBM
Blue Cross and Blue Shield of Kansas, Inc.	KAN
Blue Cross and Blue Shield of Mississippi (d.b.a. Trispan)	TRI
Blue Cross and Blue Shield of Montana, Inc.	MNT
Blue Cross and Blue Shield of Nebraska	NEB
Blue Cross and Blue Shield of Rhode Island	RHI
Blue Cross and Blue Shield of South Carolina (d.b.a Palmetto Government Benefits Administrators)	PGBA
Blue Cross and Blue Shield of Tennessee (d.b.a. Riverbend Government Benefits Administrators)	RGBA
Blue Cross and Blue Shield of Western New York, Inc. (Healthnow New York, Inc.)	HLN
Blue Cross and Blue Shield of Western New York, Inc. (Healthnow'DMERC)	HLND
Blue Cross and Blue Shield of Wyoming	WYG
Blue Cross and Blue Shield of Wisconsin (d.b.a. United Government Services, LLC)	UGS
Care First of Maryland, Inc.	CFM
Connecticut General Life Insurance Company (a CIGNA Company)	CIG
Cooperative de Seguros de Vida de Puerto Rico	COP
Empire Healthchoice, Inc. (d.b.a Empire Medicare Services)	EMP
First Coast Service Options, Inc.	FCSO
Group Health Incorporated	GHI
Group Health Service of Oklahoma, Inc. (d.b.a Blue Cross and Blue Shield of Oklahoma)	GHO
Highmark Inc. (d.b.a. HGSAdministrators)	HGSA

Contractor / System / Entity	Acronym
Highmark Inc. (d.b.a. Veritus Medicare Services)	VRT
Highmark Inc. (Data Center) Note: These letters are not identified by or nor can be found in the OFM Financial Manual. It was created specifically to be used for CISS to show ownership by the corporate structure.	HIGH
Mutual of Omaha Insurance Company	MUT
National Heritage Insurance Company	NHIC
Nationwide Mutual Insurance Company	NAT
Noridian Mutual Insurance Company	NOR
EDS Sacramento	EDS
EDS Plan	EDP
Regence Blue Cross and Blue Shield of Oregon (Medicare Northwest)	MNW
Regence Blue Cross and Blue Shield of Utah	UTAH
TrailBlazer Health Enterprises, LLC	THE
Triple S, Inc.	SSS
Wisconsin Physicians Service Insurance Corporation	WPS

- The second two digits are the last two numbers of the year of the review.
- The third one or two characters identify the type of review.

    - One character identifiers are used to identify the type of review in accordance with the *OFM Financial Manual* (see CMS Pub 100-6, Chapter7).
    - Two character identifiers are used to identify types of reviews that are not included in the *OFM Financial Manual*. These are normally requirements based on other (non-financial) Federal security requirements.

Identifier	Types of Review
In accordance with OFM Financial Manual, Chapter 7	
R	Accounts Receivable review
C	CPIC (the annual self certification package)
E	CFO EDP review
F	CFO Financial review
S	Statement on Auditing Standards number 70 (SAS70)
O	OIG reviews (HHS Office of Inspector General (Information Technology) controls assessment)
G	GAO reviews (financial reviews)
P	CMS 1522 workgroups reviews
V	CFO related NVA/ST
N	SAS 70 Novation

Identifier	Types of Review
M	CMS CPIC workgroup reviews
Not included in the OFM Financial Manual	
9T	Section 912 testing
9E	Section 912 Evaluations
AC	CMS Self-assessment Annual Compliance Audits
IR	Internal reviews initiated by the entity to meet other federal requirements
RA	Issues identified during routing risk assessments

- The last three digits are three numbers assigned to each individual finding (beginning with 001, 002, 003, etc.), for the year of the review.

Examples of material weaknesses reported in a Certification Package for Internal Controls (CPIC) over three years would be:

- ASF-03-C-001;
- ASF-03-C-002;
- CIG-04-9T-003;
- ASF-04-9E-001;
- ALA-04-9E-002;
- SSS-05-IR-002; and
- HLN-05-RA-001.

NOTE: While reporting on applications, entities and / or systems, a type of review or an entity that is not represented within the lists above may need to be created. In this case, the tester shall contact CMS for the appropriate numbering standard (acronyms or identifiers).

3.4.2 METHODOLOGY OF VULNERABILITY TESTING

The tools and test procedures used to conduct the vulnerability assessment shall be described in the "Methodology of Vulnerability Testing" sub-section. Identify whether the testing was conducted in accordance with the *CMS Information Security Testing Approach* and / or the *CMS Information Security Certification and Accreditation (C&A) Methodology*. This sub-section shall include methods of discovery such as port scanning, packet spoofing, vulnerability scanning, etc. The list of tools and the purpose of each shall be presented within a table format. Refer to this section in Appendix A for sample language and formatting.

3.4.3 METHODOLOGY OF SECURITY TEST REPORTING

The criteria for measuring the Risk Level, Ease-of-Fix, and Estimated Work Effort metrics that are included within each Business Risk shall be described in the "Methodology of Security Test Reporting" sub-section. The information contained within this sub-section shall be standard

(boilerplate) for all security testing. Refer to this section in Appendix A for the required language and formatting.

3.4.4 BUSINESS RISKS

The individual Business Risks provide technical details and analysis of each vulnerability discovered during the security test, and contains suggestions for corrective actions that will close or reduce the impact of each vulnerability. The primary audience for the Business Risks comprises System Owners, System and Network Administrators, and managers responsible for information security. Understanding that some members of this audience, such as managers, may be concerned with the middle ground between an executive overview and technical details, each Business Risk shall include mid-level metrics to describe the Risk Level, Ease-of-Fix, and Estimated Work Effort. These metrics shall be assessed based upon the guidelines presented in Section 4 of this document.

The Business Risk template is divided into one section that provides the technical details of each vulnerability, and a separate section that provides step-by-step suggestions for corrective actions. This enables CMS and contractor personnel responsible for implementing corrective actions to separate the fix from the issue, and respond directly to each corrective action suggested. Suggested corrective actions must be documented in a clear, precise manner in order to ensure reader comprehension and prevent misinterpretation.

Refer to Section 4 for guidance on how to document Business Risks. Additionally, Appendix A contains a template for Procedural Business Risks (Section 3.3 of Appendix A) and a template for Technical Business Risks (Section 3.4 of Appendix A).

3.5 REPORT APPENDICES AND ATTACHMENTS

Appendices shall be included within the report, when required or appropriate. A network, system, or application diagram illustrating the information system architecture shall be included as an appendix to all security test reports. Other appropriate appendices include:

1. The system or application test plan and test scripts when applicable;
2. List of checks performed by automated vulnerability scanning software, particularly when few or no Business Risks have been documented;
3. Screenshots demonstrating vulnerabilities documented within report.

3.6 SECURITY TEST REPORT PACKAGE

The Security Test Report Package shall be prepared by the tester in two versions: One version for the official CMS copy; one version for the system owner and, if designated by CMS, an additional copy for other responsible entities. These packages shall be delivered in hard copy and on a password-protected CD-ROM disc (see Section 5.5). The hard copy will be packaged in a clearly labeled binder with tabbed sections for the contents defined in Section 5 and Section 5.4 of this document. Note: Section 5.4 is for the official CMS version, only, and *shall not* be included in the system owner / other responsible entity package(s).

4. GUIDELINES FOR DOCUMENTING BUSINESS RISKS

Security testing is conducted to evaluate and / or validate the effectiveness of management, operational, and technical security controls implemented to protect CMS information systems. Technical or procedural vulnerabilities discovered through security testing reveal those areas where controls are not adequate, and identify the need for additional or different controls in one or more categories. To understand the significance of each vulnerability, the vulnerability must be expressed in terms of the Business Risk it will create if the associated threat materializes. Vulnerabilities, which are the direct findings of any security test, must therefore be framed in terms of the CMS Business Risk. The Business Risk shall be described in a manner to explain how the CMS business mission will be impacted if a known threat exploits an identified vulnerability and reasonable and appropriate corrective actions shall be suggested to close or reduce the impact of the vulnerability. Technical vulnerabilities will be expressed as Technical Business Risks and Procedural vulnerabilities will be expressed as Procedural Business Risks. In addition to the detailed narrative analysis, three (3) metrics are used to convey the significance of each Business Risk. These metrics are defined below. Report authors shall use this section as a guide for documenting Business Risks. Appendix A contains a template for Procedural Business Risks (Section 3.3 of Appendix A) and a template for Technical Business Risks (Section 3.4 of Appendix A).

4.1 GUIDELINES FOR ASSESSING RISK LEVEL

Vulnerabilities identified through security testing will be presented in a manner that best conveys specific risks to CMS business. A Risk Level value (**Low**, **Moderate**, or **High**) will be assigned to each risk, and will be determined by considering the threat exposure and the potential severity of the impact that would occur if the threat were to exploit the vulnerability.

Impact severity will fall into one of the following categories, which describe the potential effects on the confidentiality, integrity, and availability of information processed, stored, or transmitted by a CMS information system:

Minor	A minor impact indicates a temporary effect on the availability of non-critical information (e.g., an ICMP Denial-of-Service attack on a web server). No sensitive information is disclosed, and the integrity of information is preserved.
Significant	The availability of one of CMS's key public information systems is suspended for a limited time, rendering the service inoperable to its primary users.
Serious	The integrity of non-sensitive, non-critical information is compromised (for example, a web page is altered giving false information that misleads CMS beneficiaries). Availability of critical information systems may also be compromised for a limited time, but no sensitive information is disclosed.
Severe	Information protected by the Privacy Act of 1974, or other CMS

	sensitive but unclassified information is disclosed. The integrity and confidentiality of sensitive and critical information is compromised. Important information services may be rendered unavailable for an extended length of time.
Critical	CMS core business functions are disabled indefinitely. The integrity or availability of mission critical information is compromised. The disclosure of defense, intelligence, or national security information would have a critical impact severity if CMS possessed any such information.

The impact severity level is paired with a Threat Exposure that describes the person or event that may exploit the vulnerability, and cause harm to CMS information or information systems. The Threat Exposure shall be classified as one of the following, and if more than one threat exposure applies to a particular vulnerability, the one representing the greatest level of exposure shall be used:

Authorized Internal User	A user with an account or access to the internal system affected by the vulnerability. This user may be a CMS employee or a third party contractor or business partner who has been granted access to CMS systems.
Unauthorized Internal User	A user who has access to the building (and therefore physical access to the CMS network), but who does not have specific access privileges to the system affected by the vulnerability.
Authorized External User	An authorized external user. This may be an employee, contractor, or vendor technician working from an off-site location with access to the CMS network through a dial-up line or a virtual private network (VPN) connection.
Unauthorized External User	An unauthorized external user. This is any off-site user who attempts to access CMS information systems without the use of access privileges.
Procedural	Procedural threat exposures are non-human factors. Lack of Disaster Recovery Plans, weak password policies, and poor backup policies are examples of procedural threat exposures.

The Risk Level value contained within each Business Risk is the product of the Impact Severity Level multiplied by the Threat Exposure. The following table shall be used to calculate the Risk Level.

Risk Level Assessment Guidelines: The Risk Level of a Business Risk can be determined by matching a Threat Exposure with its Potential Impact on an information system. The derived value (intersection of these two) represents the Risk Level.

Threat Exposure	Potential Impact				
	Minor	Significant	Serious	Severe	Critical
Authorized Internal User	Low	Low	Low	Moderate	High
Unauthorized Internal User	Low	Low	Moderate	High	High
Authorized External User	Low	Moderate	Moderate	High	High
Unauthorized External User	Low	Moderate	High	High	High
Procedural	Low	Moderate	Moderate	High	High

4.2 GUIDELINES FOR ASSESSING EASE-OF-FIX

The ease with which the Business Risk can be reduced or eliminated is described using the following guidelines:

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly and without causing disruption to the system, application, or data.
Moderately Difficult	**For software / hardware**: A vendor patch or major configuration change may be required to close the vulnerability, which will likely cause a noticeable service disruption. The corrective action may require an upgrade to a different version of the software, and the re-configuration required to close the vulnerability may impact legitimate users. **For other problems**: The corrective action may require construction or significant alterations in the manner in which business is undertaken.
Very Difficult	**For software / hardware**: An obscure, hard-to-find vendor patch may be required to close the vulnerability, or significant, time-consuming configuration changes may be required. The

Rating	Definition of Ease-of-Fix Rating
	high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling. **For other problems**: The corrective action requires major construction or redesign of an entire business administrative process.
No Known Fix	**For software / hardware**: This vulnerability is due to a design-level flaw that cannot be resolved by patching or re-configuring vulnerable software. It is possible that the only way to address this problem is to cease using the software or protocol, or to isolate it from the rest of the network, thereby eliminating reliance on it. If it must be used, regular monitoring must be conducted to validate that security incidents have not occurred. **For other problems**: No known solution to the problem currently exists. Instead, all mitigating efforts to control the situation should be undertaken. It should be monitored to ensure that compromise has not occurred, and should be revisited annually to determine if a solution has been found.

4.3 GUIDELINES FOR ASSESSING ESTIMATED WORK EFFORT

The estimated time commitment required for CMS or contractor personnel to implement a fix for the Business Risk is categorized as follows:

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (roughly three days or less) is required of a single individual to complete the corrective action(s).
Moderate	Time commitments of up to several weeks are required of multiple personnel.
Substantial	Significant time is required of multiple personnel to complete the corrective action(s). Examples of substantial work efforts

Rating	Definition of Estimated Work Effort Rating
	include the redesign and implementation of CMS network architecture, and the implementation of new software with associated documentation, testing, and training across multiple CMS organizational units.
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.

Note: Under Estimated Work Effort there is also the option of estimating time duration for fixing a problem based on the level of commitment and an adequate skill set in the personnel performing the fix.

4.4 SECURITY CONTROL FAMILIES

The Business Risk shall be associated with at least one (1) of the seventeen (17) security control families described in NIST Special Publication 800-53 2nd Public Draft, *Recommended Security Controls for Federal Information Systems*. The security control families, as listed in the NIST publication, are:

1. Access Control (AC)
2. Awareness and Training (AT)
3. Audit and Accountability (AU)
4. Certification, Accreditation, and Security Assessments (CA)
5. Configuration Management (CM)
6. Contingency Planning (CP)
7. Identification and Authentication (IA)
8. Incident Response (IR)
9. Maintenance (MA)
10. Media Protection (MP)
11. Physical and Environmental Protection (PE)
12. Planning (PL)
13. Personnel Security (PS)
14. Risk Assessment (RA)
15. System and Services Acquisition (SA)
16. System and Communications Protection (SP)
17. System and Information Integrity (SI)

A deficiency in one or more of the above security control families will result in some technical or procedural vulnerability. To categorize Business Risks into security control families, the report's author shall determine which control family deficiency is the cause of the vulnerability. All security control families that directly contribute to, or permit the existence of the vulnerability shall be listed within the Business Risk. The following table provides examples of

the types of controls that are contained within each family. The security control categories in the following table are grouped into Management, Operational, and Technical controls, and do not follow the exact ordering of the NIST document, however, the categories and control types mirror the NIST guidance.

Type of Control	Security Control Family	Examples of Controls
Management Controls	RA	Risk Assessment Policy and Procedures Security Categorization Risk Assessment Risk Assessment Update
	PL	Security Planning Policy and Procedures System Security Plan System Security Plan Update Rules of Behavior Privacy Impact Assessment
	SA	System and Services Acquisition Policy and Procedures Allocation of Resources Life-Cycle Support Acquisitions Information System Documentation Software Usage Restrictions User Installed Software System Design Principles Outsourced Information System Services
	CA	C&A and Security Assessment Policy and Procedures System Assessment Information System Connections Security Certification Plan of Action and Milestones Security Accreditation Continuous Monitoring
Operational Controls	PS	Personnel Security Policy and Procedures Position Categorization Personnel Screening Personnel Termination Personnel Transfer Access Agreements Third Party Personnel Security Personnel Sanctions

Type of Control	Security Control Family	Examples of Controls
	PE	Physical and Environmental Protection Policy and Procedures Physical Access Authorizations Physical Access Control Access Control for Transmission Medium Access Control for Display Medium Monitoring Physical Access Visitor Control Access Logs Power Equipment and Cabling Emergency Shutoff Emergency Power Emergency Lighting Fire Protection Temperature and Humidity Controls Water Damage Protection Environmental Control Training Environmental Control Testing Delivery and Removal Alternative Worksite Access Control for Portable and Mobile Systems
	CP	Contingency Planning Policy and Procedures Contingency Plan Contingency Training Contingency Plan Testing Contingency Plan Update Alternate Storage Sites Alternate Processing Site Alternate Telecommunications Services Information System Backup Information System Recovery and Reconstitution
	CM	Configuration Management Policy and Procedures Baseline Configuration Configuration Change Control Monitoring Configuration Changes Access Restrictions for Change Configuration Settings

Type of Control	Security Control Family	Examples of Controls
	MA	System Maintenance Policy and Procedures Periodic Maintenance Maintenance Tools Remote Maintenance Maintenance Personnel Timely Maintenance
	SI	System and Information Integrity Policy and Procedures Flaw Remediation Malicious Code Protection Intrusion Detection Tools and Techniques Security Alerts and Advisories Security Functionality Verification Software and Information Integrity
	MP	Media Protection Policy and Procedures Media Access Media Labeling Media Storage Media Transport Media Sanitization Media Destruction and Disposal Media-related Records
	IR	Incident Response Policy and Procedures Incident Response Training Incident Response Testing Incident Handling Incident Monitoring Incident Reporting Incident Response Assistance
	AT	Security Awareness and Training Policy and Procedures Security Awareness Security Training Security Training Records

Type of Control	Security Control Family	Examples of Controls
Technical Controls	IA	Identification and Authentication Policy and Procedures User Identification and Authentication Device Identification and Authentication Identifier Management Authenticator Management Authenticator Feedback Cryptographic Module Authentication
	AC	Access Control Policy and Procedures Account Management Access and Information Flow Control Separation of Duties Least Privilege Unsuccessful Logon Attempts System Use Notification Privacy Policy Notification Previous Log-on Notification Concurrent Session Control Session Lock Session Termination Supervision and Review – Access Control Permitted Actions without Identification and Authentication Automated Marking Automated Labeling Remote Access Wireless Access Restrictions
	AU	Audit and Accountability Policy and Procedures Auditable Events Content of Audit Records Audit Storage Capacity Audit Processing Audit Monitoring, Analysis, and Reporting Audit Reduction and Report Generation Time Stamps Protection of Audit Information Non-Repudiation

Type of Control	Security Control Family	Examples of Controls
	SP	System and Communications Protection Policy and Procedures Application Partitioning System Function Isolation Information Remnants Denial-of-Service Protection Resource Priority Boundary Protection Transmission Integrity Transmission Confidentiality Network Disconnect Trusted Path Cryptographic Key Establishment and Management Cryptographic Operations Public Access Protections Collaborative Computing Transmission of Security Parameters Public Key Infrastructure Certificates Mobile Code

Complete the "Security Control Family" section of the Business Risk template by entering one or more appropriate control families.

4.5 COMMON VULNERABILITY AND EXPOSURE NUMBERS

List any Common Vulnerability and Exposure (CVE) numbers that apply to the vulnerability in the "NIST CVE #" section of the Business Risk template. CVE numbers may be obtained from vulnerability scanning tools that report by CVE, or by searching the CVE database located at "http://www.cve.mitre.org/cve/".

4.6 BUSINESS RISK DESCRIPTION

Complete the "Description" section of the Business Risk template by documenting the technical details of the vulnerability, which include: (1) How the vulnerability was discovered; (2) How the vulnerability could be exploited; (3) Who may exploit the vulnerability; (4) What systems (IP addresses) are affected by the vulnerability; and (5) The harm or damage that would occur if the vulnerability were exploited. The harm or damage that may occur if the vulnerability is exploited shall be described in terms of the business impact to CMS. Specifically, how the confidentiality, integrity, and / or availability of information may be affected and what type and sensitivity level of information is at risk of compromise.

4.7 SUGGESTED CORRECTIVE ACTION

Complete the "Suggested Corrective Action" section of the Business Risk template by documenting the remediation procedures necessary to close or reduce the vulnerability. Remediation procedures may include, but are not limited to, applying patches or service packs, upgrading hardware or software, implementing new or different controls, modifying configuration settings, or developing or modifying information security policy. The suggested corrective action shall be presented in a step-by-step approach, and each step shall be numbered. Corrective actions shall be reasonable and appropriate from a risk-based perspective, based upon the information sensitivity level, Risk Level assessment, and relevant security control families.

4.8 STATUS

The "Status" section shall include the date the Business Risk was identified, and any subsequent action taken by CMS or CMS contractors. Subsequent actions include, but are not limited to, closing or reducing the impact of the vulnerability by completing corrective actions, providing sufficient evidence to show that the vulnerability no longer exists, or performing validation testing to verify that the vulnerability no longer exists.

5. REPORT PACKAGE DOCUMENTATION

5.1 POA&M TRACKING FORM

When the final security test report is submitted to CMS, a CAP shall be developed to monitor and manage corrective actions. The CAP will assist CMS and / or Medicare Contractors in organizing information regarding Business Risks currently being addressed, the expected completion dates of corrective actions, and management's decisions to accept Business Risks and not undertake corrective actions. The POA&M Tracking Form is the instrument through which CMS and / or Medicare Contractors shall monitor corrective actions, and track the status of the CAP process. The POA&M Tracking Form is a living document, which shall be continually updated through the CAP process. The report author (testing entity) shall initially prepare the POA&M Tracking Form, and submit the completed form along with the final security test report. The POA&M Tracking Form template is included as Appendix B. Based upon the information contained in the security test report, the report author shall complete the "Findings", "Identified Weakness", "Status", "Risk Level", and "Security Control Family" columns. The CMS and / or Medicare Contractor business owners shall complete the remaining fields with the appropriate information, and will be responsible for maintaining the POA&M Tracking Form throughout the CAP process. Medicare Contractors are individually responsible for maintaining the POA&M Tracking Form for systems under their control.

5.2 ORIGINAL WORKING PAPERS SECTION

This section is for the CMS official copy only. This is not applicable for the package deliverables for the system owner and / or other responsible entities. For all other versions, continue to Section 5.5.

The purpose of an Original Working Papers Section is to accurately document the process from the beginning of the testing engagement to the report, in support of the report. In this situation, the security test plan, security test script, all documented communications and the original working papers, in a single package, are provided to SSG. This package will be specially marked as confidential information requiring special handling. The intended audience for this level of documentation is technical auditors who are assigned the task of validating the information contained within a report and assuring that the required procedures were followed during the testing and reporting process. It is crucial that a security test report is supported by the original materials package and contains no information that cannot be adequately supported by documented evidence. This enables individuals / entities reviewing the report to render informed decisions regarding the validity of the report. For this reason, it is necessary to provide all documentation leading to the report of all vulnerabilities discovered through security testing.

The following sections, listed in chronological order according to when or how they are conducted or developed, identify and describe the components of the Original Working Papers Section format. Refer to Appendix E and F for the original materials package's test plan and test script templates that shall be used to document the security testing procedures. The Original Working Papers Section will be contained within a three-ring binder, clearly labeled (cover and spine) as the Working Papers Section and display the system owner's organization's name and

location. Each section shall be divided and clearly labeled with their appropriate names: Test Plan, Test Script, Communications, Supporting Papers, and Working Papers.

5.2.1 TEST PLAN

Before the final security test report is submitted to CMS and the actual test is conducted, a test plan shall be developed to outline general testing actions, the tools utilized, the types of tests conducted, interviews, meetings and expected arrival and departure times / dates. The CMS required format for the test plan is demonstrated in the template provided in Appendix F. The test plan will assist CMS and / or Medicare Contractors in preparing to accommodate the auditor for their test and allocate resources (physical, IT and personnel) by providing the expected tests, interviews and dates of each activity. The test plan author (testing entity) shall prepare the introduction meeting agenda, the status meeting agendas and the exit meeting agenda. The meeting agendas will be documented in the communications section, described in Section 6.3. The test plan will outline all areas in which the report will address and capture the scope of the testing to be conducted. Based upon the information contained in the test plan, the report author shall report findings outside of the scope of the test plan as "observations", but will not actively pursue these areas. Observations do not impact the overall security posture of the testee, instead it assists them in mitigating risks that may impact future audits.

The test plan is reviewed by CMS and / or the entity that is subject to the testing for validating the information contained within the test plan, updating / correcting information contained within or attached to the test plan, and coordinating the logistics surrounding the testing and reporting process.

5.2.2 TEST SCRIPT

The test script shall be prepared prior to the security test in accordance to the scope of the test, to be included as part of the testing and creation processes of the working papers. The test script consists of interview questions grouped, and listed chronologically, into the 17 control families of NIST SP 800-53 and based upon those NIST controls. Each script question / criteria is to be signed and the results with optional comments recorded. Weaknesses found through the test script process, e.g. the "requirements are not met" column is checked, will be recorded within the Security Test Report and the test script shall be referenced. The test script template is included as Appendix G.

5.2.3 COMMUNICATIONS

The Communications section of the Original Working Papers Section contains the documented communications leading up to, throughout, and following the security test between the testing entity and CMS, or the combination. The type of communications to be included, but are not limited to, the following:

- E-mails;
- Meeting notes;
- Meeting agendas;
- Written voice messages;
- Facsimiles;

- Letters; and
- Delivery / courier receipts.

In the instances of electronic communications resulting in file or printing format, the communication shall be printed in its original, unaltered state. If an e-mail displays replies, from the original e-mail, then the e-mail containing the most replies can be printed instead of reprinting each individual e-mail separately, as long as all communications are captured in connection with the originating e-mail.

5.2.4 SUPPORTING PAPERS

Prior to the test plan, information will be requested of the system owner to assist in the development of the test plan. This information may include, but is not limited to, system or network diagrams, system names and addresses, contact information, past risk assessments and system security plans, and system configuration documentation. This information supports the test plan and serves as a basis for the scope and the types of tests conducted. Therefore, any information released to the tester should be included in this section. If information was not released, but reviewed on-site by the tester, it should be listed with the name, version and date of the document(s). This information shall be considered supporting documentation and included in the Supporting Papers section of the Original Working Papers Section.

During the test, vulnerability and scanning tools generate reports in electronic or hard copy format. All reports from these utilities are to be printed (when not already in hard copy format) and included within the Supporting Papers section of the Original Working Papers Section, as they support the testing process and the resulting report.

When the final security test report is submitted to CMS, a CAP is developed to monitor and manage corrective actions. Often times, as the report is being finalized, the CAPs are developed and executed. In this instance, evidence of the remediation shall be provided by the system owner and included within the Supporting Papers section of the Original Working Papers Section.

5.2.5 WORKING PAPERS

During the test, the evaluator often times will make notations in the process of validating vulnerability and scanning tool generated findings to eliminate false-positives or further provide evidence of vulnerabilities. Notations, whether related to technical tests, interviews, supporting documentation or appointments in connection with the testing will be provided in their original format in the Working Papers section of the Original Working Papers Section. Also included within the Working Papers section are written responses, questions or notations by the system owner, or SSG contact, in the presence of the tester.

5.3 CD-ROM

A password-protected CD-ROM disc shall be created as part of the security test report package. The CD-ROM shall contain the report in electronic format, the Findings Tracking form, the Weakness Summary report, and the POA&M Form (see Section 5). The CMS official copy CD-

ROM will also contain all working papers produced, created, or stored in electronic format and, if applicable, the VACAP database update. All hard-copy working papers, signed test scripts and test plans shall be included with the CMS copy of the final report package, as described in Section 3.6.

APPENDIX A – SECURITY TEST REPORT TEMPLATE

How to use this template:

Boilerplate language that shall be used in all reports is included in some sections, in others, however, certain information must be entered based upon the individual circumstances of each test. Language that must be changed for each report is included within [brackets], and is highlighted in gray. Other sections include sample language that is recommended for use in all reports, but will vary depending on the system under review.

The Cover Page contains boilerplate information that shall be included within all reports.

Section 1, Introduction, contains sample language that shall be used when appropriate. Based upon the circumstances of the testing engagement, the report author shall supplement or modify the sample language.

Section 2, Executive Summary, does not contain sample language. This section contains instructions for the types of information that shall be included within the Executive Summary.

Section 3.0, Detailed Findings, contains boilerplate language that shall be included within all reports.

Section 3.1, Methodology for Vulnerability Assessment, contains sample language that shall be used in all reports, where appropriate. This language, however, will change based upon the scope of testing and test procedures.

Section 3.2, Methodology for Security Test Reporting, contains boilerplate language that shall be included within all reports.

Sections 3.3 and 3.4 contain boilerplate language that should be included within all reports.

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES

Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

[System Name & Acronym]
[Type of Review]

Version # click here and enter version # (follow with DRAFT if appropriate)
click here and enter date of this version of the DOCUMENT (not an autodate)
Template July 15, 2005 - Version 4.0

TABLE OF CONTENTS

1. INTRODUCTION 1
2. EXECUTIVE SUMMARY 2
3. DETAILED FINDINGS 3
3.1 Methodology for Vulnerability Assessment 4
3.2 Methodology for Security Test Reporting 6
3.2.1 Risk Level Assessment 6
3.2.2 Ease-of-Fix Assessment 7
3.2.3 Estimated Work Effort Assessment 8
3.3 Procedural Business Risks (If any were identified) 10
3.3.1 Business Risk: 11
Click here and type Business Risk Title 11
3.4 Technical Business Risks 12
3.4.1 Business Risk: 13
Click here and type Business Risk Title 13

1. INTRODUCTION

Important: This section of the template includes sample language that should be used in actual security test reports, where appropriate. Language that must be changed for each report is included within [brackets], and is highlighted in gray. It is expected that some variation from the sample language below will be necessary, depending on the system or application under review.

The Centers for Medicare & Medicaid Services (CMS) of the United States Department of Health & Human Services engaged [Contractor] to perform remote and on-site vulnerability assessment of the [System or Application Name] as part of its [Contract Title]. CMS issued a vulnerability testing methodology as part of the task order, and [Contractor] combined all aspects of this methodology with internal proprietary methods to offer comprehensive vulnerability assessment. Remote testing was performed [Dates] and on-site testing was performed at the [Location] on [Dates].

[Contractor] conducted security testing and configuration review of the web and database servers. The target web server is designed for limited public access, and the database server to be used only by authorized administrators with proper authentication. [Contractor] employed operating system commands, research, technical tools, and manual processes to execute the test plan designed for this task. The test plan developed by [Contractor] was reviewed and authorized by CMS staff prior to the start of testing. Attachment 1 to this report illustrates the [System or Application Name] network design.

Networks, systems, and applications within the CMS internal environment store, process, and transmit sensitive personal information, and accordingly the confidentiality requirements are strict. The vulnerability assessment process is one portion of an overall information security program to ensure the CMS information infrastructure operates securely, and resists attacks that attempt to compromise sensitive information, and / or cause harm to CMS' computer and network resources. This report presents the vulnerability assessment findings.

DRAFT Report

2. EXECUTIVE SUMMARY

Important: This section of the template includes instructions for what types of information shall be documented within the Executive Summary. This is NOT sample language or boilerplate language.

The Executive Summary shall:

1. Describe the purpose of system or application under review, including a description of the business function supported by the system or application;
2. Describe the project background, including who requested and authorized the security test;
3. Provide a brief statement of scope for the security testing engagement;
4. Identify who is authorized to access the system or application; and
5. Identify the information security requirements and any special security concerns associated with the system or application.
6. Identify any observations of any security vulnerabilities beyond the scope of the test in a narrative form.

The Executive Summary shall also, at a high level:

1. Describe the test procedures that were conducted;
2. Identify from where the testing was conducted;
3. Describe the major vulnerabilities identified; and
4. Briefly discuss the need for any immediate or significant corrective actions.

The business impact of each major vulnerability shall be stressed to ensure that the reader understands the significance of the issue, and is in the position to render an informed risk-based decision. The total number of findings identified during the test, represented as Business Risks, shall be documented within this section, as well as an assessment as to how difficult it will be to address the majority of open issues. The Executive Summary should particularly address any policy-level issues that persist throughout the CMS environment, and any strategic options to address categorical weaknesses.

DRAFT Report

3. DETAILED FINDINGS

Important: This section of the template includes boilerplate language that shall be used in all security test reports. Language that must be changed for each report is included within [brackets], and is highlighted in gray. The final paragraph and bullets shall be deleted if no vulnerabilities beyond the scope of the test are identified.

This section provides descriptive analysis of the vulnerabilities identified through the [vulnerability assessment or ST&E] process. Each vulnerability is thoroughly explained, specific risks to the continued operations of the CMS information systems are identified, and the impact of each risk is analyzed as a business case. The Business Risks also contain suggested corrective actions for closing or reducing the impact of each vulnerability.

Preceding the detailed findings categorized as Procedural Business Risks in section 3.3 and Technical Business Risks in section 3.4, the methodologies for performing vulnerability assessment and reporting test results are presented in section 3.1 and 3.2, respectively. These sections explain the vulnerability testing process, and describe how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been assessed.

During the course of the [vulnerability assessment or ST&E] process, the following vulnerabilities were identified, but are out of scope:

- [Vulnerability description in a brief narrative statement]
-

3.1 METHODOLOGY FOR VULNERABILITY ASSESSMENT

Important: This section of the template includes sample language that should be used in actual security test reports, where appropriate. Language that must be changed for each report is included within [brackets], and is highlighted in gray. It is expected that some variation from the sample language below will be necessary, depending on the system or application under review. This is particularly true for the list of tests that were conducted and the lists of tools used.

To complete the requirements of the CMS task order, [Contractor or CMS] followed the [*CMS Information Security Testing Approach* **and** / **or** *CMS Information Security Certification and Accreditation (C&A) Methodology*]. These methods were combined with [Contractor's] internal security testing methodologies to offer a comprehensive vulnerability assessment. Both commercially available and freeware vulnerability identification tools were employed, as well as operating system commands, vulnerability research at security web sites, and manual processes.

To support the [*CMS Information Security Testing Approach* **and** / **or** *CMS Information Security Certification and Accreditation (C&A) Methodology*], the following were performed:

1. Attempts to access internal network hosts, including the mainframe, using common and default user accounts and passwords.
2. Obtaining a TSO user account with no dataset access privileges, viewing the user account capabilities, and identifying sub-systems present in the configuration.
3. Attempts to invoke the security package within MVS mainframes.
4. Attempts to set up a new power user or super user account within MVS mainframes.
5. Attempts to alter security software parameters within MVS mainframes.
6. Scan for sensitive or confidential information in the JES2 output spool.
7. Attempts to access various sensitive Medicare data sets from menu 3.4 of ISPF.
8. Automated vulnerability scanning comparable to ISS Internet Scanner policy level L1-L2. This process was completed using Nessus Security Scanner. JANUS performed vulnerability scans at levels comparable to, and greater than levels L1 and L2.
9. Attempts to gain password files and passwords hashes using network-sniffing applications.
10. Use of password cracking applications to discover valid passwords from encrypted password files, or through brute force log-on attempts.
11. Attempts to create false trust relationships and access network user lists using vendor security tools.
12. Penetration testing of internal networks, systems, and applications that store, process, or transmit Medicare information. This was performed for the systems identified by CMS, including mid-tier systems, database servers, e-mail servers, file servers, the DMZ environment, network firewalls, routers, and switches.
13. Internal network security testing involving manual procedures for all of the systems listed in item 12.

14. Tests to determine CMS's internal intrusion detection capability. These tests included port scans, vulnerability scans, password cracking attempts, and manual vulnerability exploitation.

To complete the technical security testing, [Contractor **or** CMS] implemented the following programs, tools, utilities, and operating system commands (all testing procedures within the Testing Purpose column refer to the previous list):

Vendor	Product/Command	Testing Purpose
Open Source	Nessus Security Scanner	Automated vulnerability scanning to support testing procedures 1, 8, 12, and 14.
JANUS Associates, Inc.	I.C.U….MVS	Automated vulnerability assessment of MVS mainframes, to support testing procedures 1, 2, 3, 4, 5, 6, and 7.
Open Source	Nmap	Port scanning, to support testing procedures 8, 12, 13, and 14.
Foundstone	SuperScan	Port scanning, to support testing procedures 8, 12, 13, and 14.
Open Source	Pandora's Box	Novell vulnerability assessment, to support testing procedures 1, 8, 10, 11, 12, 13, and 14.
@Stake, Inc.	L0phtCrack	Windows NT password hash cracking, to support testing procedures 9 and 10.
Open Source	John the Ripper	Unix password hash cracking, to support testing procedure 10.
Open Source	Novell Password Cracker	Novell password file and remote log-on cracking, to support testing procedures 1 and 10.
Open Source	Brutus	Brute force password cracker for remote log-on, to support testing procedures 1 and 10.
Cerberus Information Security, Ltd.	Nbtdump	Windows NT remote information gathering, including user accounts, password policy, share information, to support testing procedures 1, 11, 12, and 13.
Red Hat, Inc.	"snmpwalk"	SNMP information gathering, to support testing procedures 12 and 13.
Red Hat, Inc.	"host"	DNS zone transfer information, to support testing procedures 12 and 13.
Red Hat, Inc.	"ping"	Active host enumerate, to support testing procedures 12 and 13.

DRAFT Report

3.2 METHODOLOGY FOR SECURITY TEST REPORTING

Important: This section of the template includes boilerplate language that shall be used in all security test reports. Language that must be changed for each report is included within [brackets], and is highlighted in gray.

The format and content of this report has been developed in accordance with the *CMS Reporting Standard for Information Security Testing*. The CMS Reporting Standard requires that a Risk Level assessment value be assigned to each Business Risk, in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability. Based on an understanding of the vulnerabilities identified, CMS' current implementation of the underlying technology, and the assessment guidelines contained with the CMS Reporting Standard document, [Contractor **or** CMS] has assigned these values to each Business Risk.

3.2.1 RISK LEVEL ASSESSMENT

Each Business Risk has been assigned a Risk Level value of High, Medium, or Low Risk. The rating is, in actuality, an assessment of the priority with which each Business Risk shall be viewed. The following definitions apply to the Risk Assessment values:

Rating	Definition of Risk Rating
High Risk	Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS. Significant political, financial, and / or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited.
Medium Risk	Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and / or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur. OR,

	The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.
Low Risk	Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur. OR, The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal.

3.2.2 EASE-OF-FIX ASSESSMENT

Each Business Risk has been assigned an Ease-of-Fix value of Easy, Moderately Difficult, Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions, required to close or reduce the impact of the vulnerability. The following definitions apply to the Ease-of-Fix values:

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly and without causing disruption to the system, application, or data.
Moderately Difficult	**For software / hardware**: A vendor patch or major configuration change may be required to close the vulnerability, which will likely cause a noticeable service disruption. The corrective action may require an upgrade to a different version of the software, and the re-configuration required to close the vulnerability may impact legitimate users. **For other problems**: The corrective action may require construction or significant alterations in the manner in which business is undertaken.

Rating	Definition of Ease-of-Fix Rating
Very Difficult	**For software / hardware**: An obscure, hard-to-find vendor patch may be required to close the vulnerability, or significant, time-consuming configuration changes may be required. The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling. **For other problems**: The corrective action requires major construction or redesign of an entire business administrative process.
No Known Fix	**For software / hardware**: This vulnerability is due to a design-level flaw that cannot be resolved by patching or re-configuring vulnerable software. It is possible that the only way to address this problem is to cease using the software or protocol, or to isolate it from the rest of the network, thereby eliminating reliance on it. If it must be used, regular monitoring must be conducted to validate that security incidents have not occurred. **For other problems**: No known solution to the problem currently exists. Instead, all mitigating efforts to control the situation should be undertaken. It should be monitored to ensure that compromise has not occurred, and should be revisited annually to determine if a solution has been found.

3.2.3 ESTIMATED WORK EFFORT ASSESSMENT

Each Business Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. The following definitions apply to the Estimated Work Effort values:

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time (roughly three days or less) is required of a single individual to complete the corrective action(s).

Rating	Definition of Estimated Work Effort Rating
Moderate	Time commitments of up to several weeks are required of multiple personnel.
Substantial	Significant time is required of multiple personnel to complete the corrective action(s). Examples of substantial work efforts include the redesign and implementation of CMS network architecture, and the implementation of new software with associated documentation, testing, and training across multiple CMS organizational units.
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.

DRAFT Report

3.3 PROCEDURAL BUSINESS RISKS (IF ANY WERE IDENTIFIED)

Important: This section of the template includes boilerplate language that shall be used in all security test reports. Language that must be changed for each report is included within [brackets], and is highlighted in gray. All sections of the Business Risk template on the following page shall be completed according to the test results of each individual system or application.

Procedural vulnerabilities representing risks to the secure operation of [System Name] are detailed as findings in this section (e.g., policies, procedure and management and operational controls). All Business Risks within this section are procedural in nature, and will not result directly in unauthorized access. These have been separated from technical vulnerabilities that may result in unauthorized access.

The vulnerabilities are ordered in a format that will enable CMS to develop an efficient and workable action plan to remediate all risks. The Business Risks are ordered first by Risk Level, from highest risk to lowest risk level, and then by Estimated Work Effort, from Low to High. This format will help CMS to identify critical risks that shall be addressed immediately with little time and effort.

DRAFT Report

3.3.1 BUSINESS RISK:	**CLICK HERE AND TYPE BUSINESS RISK TITLE**

NIST CVE#: Click here and type CVE Identifier

NIST Security Control Family: Click here and enter Security Control Family(ies)

Risk Level: (Risk Level is High Risk, Medium Risk, or Low Risk

Click here and enter Risk Level

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Click here and enter Ease-Of-Fix

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Click here and enter Estimated Work Effort

Description:

Click here and type Description

Suggested Corrective Action(s):

1. Click here and type Corrective Action Step

Status:

Click here and type Status

3.4 TECHNICAL BUSINESS RISKS (IF ANY WERE IDENTIFIED)

Important: This section of the template includes boilerplate language that shall be used in all security test reports. Language that must be changed for each report is included within [brackets], and is highlighted in gray. All sections of the Business Risk template on the following page shall be completed according to the test results of each individual system or application.

Technical vulnerabilities representing risks to the secure operation of [System Name] are detailed as findings in this section (e.g., system implementation procedures and / or controls, and configuration procedures and / or controls). All Business Risks within this section are technical in nature, and may result directly in unauthorized access. These have been separated from procedural vulnerabilities that will not result in unauthorized access.

The vulnerabilities are ordered in a format that will enable CMS to develop an efficient and workable action plan to remediate all risks. The Business Risks are ordered first by Risk Level, from highest risk to lowest risk level, and then by Estimated Work Effort, from Low to High. This format will help CMS to identify critical risks that shall be immediately addressed with little time and effort.

DRAFT Report

3.4.1 BUSINESS RISK:	**CLICK HERE AND TYPE BUSINESS RISK TITLE**

NIST CVE#: Click here and type CVE Identifier

NIST Security Control Family: Click here and enter Security Control Family(ies)

Risk Level: (Risk Level is High Risk, Medium Risk, or Low Risk)

Click here and enter Risk Level

Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)

Click here and enter Ease-Of-Fix

Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

Click here and enter Estimated Work Effort

Description:

Click here and type Description

Suggested Corrective Action(s):

1. Click here and type Corrective Action Step

Status:

Click here and type Status

APPENDIX B –
POA&M INSTRUCTIONS AND TRACKING FORM

The following instructions explain how the POA&M Tracking Form/Excel spreadsheet should be completed. The initial completion of the Form will require more information then the periodic updates/status reports. Information must be entered in columns 2, 3, 4, 5, 8, and 9 for each reported finding for the initial submission. Once the initial POA&M has been completed, submitted to, and accepted by CMS, no changes may be made to the data in columns 1, 3, 4, 5, 7 and 10. Only columns 6, 8, 9 may be updated for the periodic reporting in the CISS tool.

Column 1- Weakness. The description of the detailed finding identified in the Data Center Findings Report will be pre-filled in this column. Sensitive descriptions of specific findings are not necessary, but sufficient data must be provided to permit oversight and tracking.

Column 2 –POC. Identity the position, title or organizational entity that the contractor/data center head will hold responsible for resolving the finding. Do not use a person's name.

Column 3 –Resources Required. Estimated staff time in hours required to resolve the finding.

Column 4 – Scheduled Completion Date. Scheduled completion date (mm/dd/yy) for resolving the finding. Please note that the initial date entered may not be changed. If a finding is resolved before or after the originally scheduled completion date, the contractor should note the actual completion date in Column 9, "Comments."

Column 5 –Milestones with Completion Dates. Key milestones with completion dates. A milestone will identify specific requirements or key steps to correct an identified finding. If the finding has two or more identified issues or elements contributing to the overall finding, the milestones and completion dates must be comprehensive enough to address all elements of the finding. Please note that once entered on the POA&M Form the initial milestones and the associated completion dates may not be altered. If there are changes to any of the milestones and/or associated scheduled completion dates the contractor/data center should note them in the column 6, "Changes to Milestones" and provide a reason for the change in column 9, "Comments."

Column 6 –Changes to Milestones. This column would include new scheduled completion dates for a particular milestone or the overall finding. The reason for the change must be recorded in column 9, "Comments."

Column 7 –Identified. The individual finding numbers from the Data Center Findings Report will be entered (pre-filled).

Column 8 –Status. The only Entries Permitted are "on-going", "delayed" or "completed." If "delayed", an entry must be made in column 6, and the reason recorded in column 9. If "completed", the completion date must be entered in column 9.

Column 9 – Comments. Record a brief summary of the work accomplished during the reporting period. An entry is also required if a scheduled completion date or milestones date is missed (record the reason) or if the finding has been corrected and all work is deemed "completed" (record the date of completion). Record any additional details or clarification for any previous entries.

Column 10 - Risk Level. This is the risk level assigned to the finding by the reviewer (pre-filled).

1	2	3	4	5	6	7	8	9	10
Weakness	**POC**	**Resources**	**Scheduled Completion Date**	**Milestones Completion Dates**	**Changes to Milestones**	**Identified**	**Status**	**Comments**	**Risk Level**

DRAFT Report

APPENDIX C –TEST PLAN TEMPLATE

C.1 YR1 ST&E TEST PLAN TEMPLATE

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

[System Name & Acronym]
YR1 ST&E
Test Plan

Draft/Final
Date
Template July 15, 2005 - Version 4.0

DRAFT Report

Table of Contents

Pre -Visit 1
On-site Visit 1
On-site Preparation 2
Start of On-site Review, Evaluation and Validation 6
Analysis and Documentation 7
Attachment 1 – (Enclosure 1 Supplement) On-site ST&E Requirement Checklist 8
Attachment 2 –Servers for Control Review 10
Attachment 3 – Timeframe and Schedule 11
Attachment 4– On-Site Technical Staff Requirements 12

DRAFT Report

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
	Pre -Visit				
		1.) Review i.e., Data Center provided SSP, RA, policies, procedures, plans and diagrams. Formulate Test Plan and Test Scripts / Protocols.			
		2.) Review Test Plan and Test Scripts / Protocols and revise for agreement and requirements.			
		3.) Inventory following credentials, documentation &/or arrangements: i.) Site-specific permits ii.) Access media iii.) Parking permits iv.) Property passes v.) Hotel Information vi.) Directions vii.) Meeting schedules			
		4.) Contact the point of contact at the Data Center to open channel of communication.			
		5.) Test Plan / Scripts / Protocols discussion with the Data Center technical points of contact: a.)Verify validity of samples for control review process:			
		i.) Servers			
		See Attachment 2			
	On-site Visit	Timeframe and Schedule			
		1.) See Attachment 3			

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
	On-site Preparation				
		1.) Validate that the following have been provided in hard-copy for review, evaluation and validation:			
		a.) System Security documentation			
		b.) Access control policies and Procedures			
		c.) Awareness and Training policies and Procedures			
		d.) Audit and Accountability policies and Procedures			
		e.) Certification, Accreditation, and Security Assessment policies and procedures			
		f.) Configuration Management policies and procedures			
		g.) Contingency Planning policies and Procedures			
		h.) Identification and Authentication policies and procedures			
		i.) Incident Response policies and Procedures			
		j.) System Maintenance policies and Procedures			
		k.) Media Protection policies and Procedure			
		l.) Physical and Environmental protection policies and procedures			
		m.) Security Planning policies and Procedures			
		n.) Personnel Security policies and Procedure			
		o.) Risk Assessment policies and Procedure			
		p.) System and Services Acquisition			

DRAFT Report

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
		policies and procedure			
		q.) System and Communications policies and procedure			
		r.) System and Information Integrity policies and procedure			
		s.) Sites' Systems Security Plan (SSP):			
		t.) Risk Assessment (RA)			
		u.) Recent security audit reports (within twelve (12) months of site visit)			
		v.) Vulnerabilities tracking records and follow-up forms and / or procedures			
		w.) Configuration Management tracking reports and / or forms			
		x.) Contingency Plan			
		y.) Disaster Recovery Plan			
		z.) Rules of Behavior			
		aa.) Privacy Impact Assessment			
		bb.) Help Desk procedures			
		2.) Mainframe configuration information to include but not limited to:			
		a.) Security packaging versions			
		b.) Operating systems and versions			
		3.) Schedule interviews for Local Administrators :			
		a.) *See Attachment 4*			
		4.) Alert key personnel in CMS and Data Center that evaluation will commence:			
		a.) CMS GTL *<Place holder for CMS GTL contact*			

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
		information > Name: Title: Name of Organization: CMS Address:7500 Security Blvd City, State, Zip Code: Balto. MD 21244 E-mail Telephone Number:			
		b.) CMS C&A Evaluator: *<Place holder for CMS Evaluator contact information>* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		c.) Network Data Center Administrator *<Place holder for Data Center Network Administrator contact information >* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		d.) System Security Officer *<Place holder for System Security Officer contact information >* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address:			

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
		Telephone Number:			
		e.) Site Team Lead *<Place holder for Site Team Lead contact information>* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		f.) System Administrator (What is the difference between system admin and network admin? *<Place holder for the System Administrator contact information>* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		g.) Facility Manager *<Place holder for the Facility Manager contact information>* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		g.) Human Resource Manager *<Place holder for the Human Resource Manager contact information>* Name:			

DRAFT Report

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
		Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		5.) Validate the following have been provided (for e-mail, printing etc.):			
		a.) Local User Account w/ password			
		6.) Validate that Admin personnel are present to verify and validate controls:			
		a.) *See Attachment 4*			
	Start of On-site Review, Evaluation and Validation				
	Review of Data Center documented security controls including, but not limited to:				
		1.) Verify security policies			
	Review Operating System Configuration: • *Review controls against sample servers*	1.) Security policy			
		2.) Audit policy			
		3.) Service pack level			
		4.) Audit log settings			
		5.) User account management			
		6.) Virus protection			
	Review Application Configurations: • *Review controls against*	1.) Evaluate application security implementation:			

Expected Timeframe	Review Process	Procedures and Methods	CONTRACTOR Tester	POC / Roles	Status
	sample servers				
		a. Internal web servers			
		b.) E-mail servers			
	Network Configuration Review:	1.) Review network architecture:			
		2.) IDS			
	Analysis and Documentation				
	Compile Findings and Generate Detailed Report:	1.) Analysis/Develop findings report:			
		a.) Evaluate risk of found vulnerabilities			
		i.) Assess risk to CMS mission			
		ii.) Consider industry standard practices and CMS ARS BPSSM, NIST, FISCAM and CSRs			
		b.) Evaluate ease-of- fix for each finding			
		c.) Present detailed findings			
		d.) Detail recommendations for mitigating or eliminating vulnerabilities			
		2.) Quality Assurance			
TBD		3.) Produce and submit draft report			
TBD		4.) Draft report discussion w/ Data Center technical staff and CMS			
TBD		5.) Review CMS comments and make changes to draft report			
TBD		6.) Produce final report			
TBD		7.) Submit final report			

ATTACHMENT 1 – (ENCLOSURE 1 SUPPLEMENT) ON-SITE ST&E REQUIREMENT CHECKLIST

REC'D	ITEM DESCRIPTION
	On-site Contact Information:
	Technical/security POCs' names and contact information
	Site Team Lead, Site Security POC and Site CMS-contract Lead names and contact information
	On-site meeting setup requirements:
	Scheduled In-Brief meeting (Pre-visit-teleconference meeting): ▪ Time, location and duration ▪ List of attendees ▪ Attendee contact information (e-mail, title, phone number, division)
	Scheduled Individual meetings (Progress report and needs analysis meeting): ▪ Time, location and duration ▪ Contact information (e-mail, title, phone number, division)
	Scheduled Status meeting
	Scheduled Out-Brief meeting: ▪ Time, location and duration ▪ List of attendees ▪ Attendee contact information (e-mail, title, phone number, division)
	On-site Administrative Requirements:
	On-site permits and access media; Parking & building access, property passes
	A room, cubicle or space to be used solely by CONTRACTOR personnel when they arrive
	If it is a room, it should have a lockable door with key(s). If a cubicle, one of the desks or tables has a lock & key, or a lockable cabinet, so that CONTRACTOR personnel can secure sensitive Client and/or CONTRACTOR materials. In the room, two desks or tables for

REC'D	ITEM DESCRIPTION
	computers and documentation review
	Room has two (2) network connections with Internet for CONTRACTOR staff personnel laptops, **in addition** to the connections supplied with existing two desktop machines (View electronic files, E-mail, printing, internet etc.,)
	IP address either supplied by DHCP or statically assigned for the Evaluators laptops
	The desktops are configured with standard software; i.e., operating systems, MS Office or equivalent (View electronic files, E-mail, note taking, printing, internet etc.,)
	A printer availability
	One set of domain/network/mid-range user IDs ▪ Least user rights/privileges (for printing, e-mail, internet etc.)
	Room has one phone and phone line
	Security and employee documentation to be stored in the lockable container, for CONTRACTOR staff review and reference during the visit

ATTACHMENT 2 –SERVERS FOR CONTROL REVIEW

Server Name	IP address	Description

ATTACHMENT 3 – TIMEFRAME AND SCHEDULE

Timeframe and Schedule		
Day 1	**Day 2:**	**Day 3:**
In-Brief Meeting at 9 AM	Daily Status Meeting	Daily Status Meeting
Conduct walk through		
Daily Status Meeting		
Day 4: Audit and Accountability, Risk Assessment	**Day 5:TBD**	**Additional Days: TBD (if needed)**
Daily Status Meeting	Wrap-up	TBD
	Final Out-Brief	TBD
		TBD
		TBD
		TBD
		TBD
		TBD

Note: This schedule may vary depending on work load.

ATTACHMENT 4– ON-SITE TECHNICAL STAFF REQUIREMENTS

Staff	Day 1 (mm/dd/yy)	Day 2 (mm/dd/yy)	Day 3 (mm/dd/yy)	Day 4 (mm/dd/yy)	Day 5 (mm/dd/yy)
Program Manager					
Network Administrator					
System Administrator					
Database Administrator					
Web Developers					
Application Developers					
Information Security Officer					
Facility Manager					
Human Resources Manager					

Note: Please check off the appropriate day for availability of technical staff.

DRAFT Report

C.2 YR2 ST&E TEST PLAN TEMPLATE

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N2-14-26
Baltimore, Maryland 21244-1850

CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS)

Office of Information Services (OIS)
Systems Security Group (SSG)
7500 Security Blvd
Baltimore, MD 21244-1850

[System Name & Acronym]
YR2 ST&E
Test Plan

Draft/Final
Date
Template July 15, 2005 – Version 4.0

DRAFT Report

Table of Contents

PRE -VISIT 1
ON-SITE VISIT 1
ANALYSIS AND DOCUMENTATION 7
ATTACHMENT 1 – (ENCLOSURE 1 SUPPLEMENT) ON-SITE ST&E REQUIREMENT CHECKLIST 9
ATTACHMENT 2 –SAMPLE SYSTEMS FOR CONTROL REVIEW 10
ATTACHMENT 3 –SCHEDULE 11
ATTACHMENT 4– ON-SITE TECHNICAL STAFF AVAILABILITY REQUIREMENTS ... 12

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
	Pre -Visit				
		1.) Prepare and submit introduction letter to Data Center with rules of engagement, schedule and request for pre-visit documentation.	.	CMS GTL	
		2.) Conduct introduction call for all Data Centers.		CMS GTL	
		3) Data Center specific introductory call. a.) Site visit overview b.) Logistics c.) Schedule / Timeline	.	CMS GTL	
		4.) Review Data Center provided SSP, RA, policies, procedures, plans and diagrams.			
		5.) Formulate Data Center test plan from the standard template.			
		6.) Participate in Data Center conference call to gather specific details to customize test plan. a.) Finalize Logistics: (See Attachment 1) i.) Site-specific permits ii.) Access media iii.) Parking permits iv.) Property passes v.) Hotel Information vi.) Directions vii.) Meeting schedules b.) Identify sample systems for verification of controls. (See Attachment 2)	.	CMS GTL	
		7.) Submit final test plan to Data Center.	.		
	On-site Visit	Schedule (See Attachment 3)			
DAY 1	*In-Brief Meeting: 9 AM*	1.) Conduct on-site preparation:	ST&E Evaluators	CMS GTL	
5/23/2005		a.) Introduce CMS, [Contractor] Personnel and confirm the availability of key personnel in Data Center. (See	ST&E Evaluators		

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
		Attachment 4)			
		i.) CMS GTL *<Place holder for CMS GTL contact information>* **Name:** **Title:** **Name of Organization:** CMS **Address:** 7500 Security Blvd **City, State, Zip Code:** Baltimore, MD 21244 **E-mail Address:** **Telephone Number:**			
		ii.) CMS ST&E Evaluator *<Place holder for CMS ST&E Evaluator contact information>* **Name:** **Title:** **Name of Organization:** **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		iii.) System Security Officer *<Place holder for System Security Officer contact information >* **Name:** **Title:** **Name of Organization:** **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		iv.) Site Team Lead *<Place holder for System Team Lead contact information>* **Name:** **Title:**			

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
		Name of Organization: **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		v.) System Administrator *<Place holder for the System Administrator contact information>* **Name:** **Title:** **Name of Organization:** **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		vi.) Data Center Network Administrator *<Place holder for Data Center Network Administrator contact information >* **Name:** **Title:** **Name of Organization:** **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		vii.) Database Administrator *<Place holder for Data Center Network Administrator contact information >* **Name:** **Title:** **Name of Organization:** **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		viii.) Facility Manager			

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
		<Place holder for the Facility Manager contact information> **Name:** **Title:** **Name of Organization:** **Address:** **City, State, Zip Code:** **E-mail Address:** **Telephone Number:**			
		ix.) Human Resource Manager *<Place holder for the Human Resource Manager contact information>* Name: Title: Name of Organization: Address: City, State, Zip Code: E-mail Address: Telephone Number:			
		b.) Validate the local user accounts w/ passwords have been provided (for e-mail, printing etc.):	ST&E Evaluators		
		2.) Participate in a walkthrough of the Data Center.	ST&E Evaluators		
	Security Planning (SP)	1.) If necessary, review and analyze SP documents that are only available on-site.	ST&E Evaluators		
		2.) Review and validate SP policies.	ST&E Evaluators		
		3.) Conduct SP interviews.	ST&E Evaluators		
	Daily Status Meeting	4.) Discuss testing status with appropriate Data Center personnel.	ST&E Evaluators .	**CMS GTL**	
DAY 2	*Contingency Planning (CP)*	1.) If necessary, review CP documents that are only available on-site.	ST&E Evaluators		
		2.) Review and validate the CP is consistent with documentation.	ST&E Evaluators		

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
		3.) Conduct CP interviews.	ST&E Evaluators		
	Daily Status Meeting	4.) Discuss testing status with appropriate Data Center personnel.	ST&E Evaluators	**CMS GTL**	
DAY 3	*Configuration Management (CM)*	1.) If necessary, review CM documents that are only available on-site.	ST&E Evaluators		
		2.) Review and validate that CM process is consistent with the documentation to ensure compliance including, but not limited to: a.) Configuration change control b.) Monitoring configuration changes	ST&E Evaluators		
		3.) Review logs for access attempts.	ST&E Evaluators		
		4.) Review and validate operating system configuration including, but not limited to: a.) Service pack level b.) User account management c.) Security applications	ST&E Evaluators		
		5.) Evaluate application configuration implementation including, but not limited to: a.) Internal web servers b.) E-mail servers c.) Mainframe	ST&E Evaluators		
		6.) Review and validate a sample of system configuration and security controls.	ST&E Evaluators		
		7.) Conduct CM interviews.	ST&E Evaluators		
	System Information Integrity (SI)	8.) If necessary, review SI documents that are only available on-site.	ST&E Evaluators		
		9.) Review and validate that SI process is consistent with documentation to ensure compliance.	ST&E Evaluators		

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
		10.) Review and validate the following are used and maintained: a.) Virus protection b.) Flaw remediation c.) Malicious code protection d.) Intrusion detection tools and techniques e.) Security alerts and advisories f.) Software and information integrity tools	ST&E Evaluators		
		11.) Conduct SI interviews.	ST&E Evaluators		
	Daily Status Meeting	12.) Discuss testing status with appropriate Data Center personnel.	ST&E Evaluators	**CMS GTL**	
DAY 4	*Audit and Accountability (AU)*	1.) If necessary, review AU documents that are only available on-site	ST&E Evaluators		
		2.) Review and validate AU process including but not limited to the following: a.) Auditable events b.) Audit log settings c.) Content of audit records d.) Audit storage capacity e.) Audit monitoring, analysis and reporting f.) Protection of audit information	ST&E Evaluators		
		3.) Conduct audit and Accountability interviews	ST&E Evaluators		
	Risk Assessment (RA)	4.) If necessary, review RA documents that are only available on-site	ST&E Evaluators		
		5.) Review and validate the RA including but not limited to the following: a.) Security categorization b.) RA document methodology c.) RA update process	ST&E Evaluators		
		6.) Conduct RA interviews.	ST&E Evaluators		

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
	Daily Status Meeting	7.) Discuss testing status with appropriate Data Center personnel.	ST&E Evaluators	**CMS GTL**	
DAY 5	*Out Brief*	1.) Provide an overview of the week's testing to appropriate Data Center personnel.	ST&E Evaluators	**CMS GTL**	
		2.) Review "Tentative" findings.	ST&E Evaluators	**CMS GTL**	
		3.) Discuss next steps including expected due dates.	ST&E Evaluators	**CMS GTL**	
		4.) Identify and document any action items.	ST&E Evaluators	**CMS GTL**	
		5.) Address any final questions.	ST&E Evaluators	**CMS GTL**	
ADDITIONAL DAYS : TBD					
	Analysis and Documentation				
	*Compile Findings and Generate Detailed Report***:**	1.) Analyze and develop findings report: a.) Evaluate vulnerabilities/threats to determine risk. i.) Assess risk to CMS mission. ii.) Consider industry standard practices and CMS ARS, PSSM, FISCAM and CSRs. b.) Document detailed findings. c.) Define recommendations for mitigating or eliminating vulnerabilities. d.) Determine ease-of- fix for each finding.	ST&E Evaluators		
		2.) Perform quality assurance tasks.	Q&A		
10 days		3.) Produce and submit draft report to CMS.	ST&E Evaluators	**CMS GTL**	

Expected Timeframe	Review Process	Procedures and Methods	[CONTRACTOR] Tester	POC / Roles	Status
TBD		4.) Conduct draft report discussion w/ Data Center technical staff.	ST&E Evaluators	**CMS GTL**	
10 days		5.) Receive comments from CMS and Data Center.		**CMS GTL**	
5 days		6.) Review CMS comments and make changes to draft report.		**CMS GTL**	
5 days		7.) Produce final report and submit to CMS	ST&E Evaluators	**CMS GTL**	

Attachment 1 – (Enclosure 1 Supplement) On-site ST&E Requirement Checklist

Rec'd	Item Description
	On-site Contact Information:
	Appropriate POCs' names and contact information.
	On-site meeting setup requirements:
	Schedule In-Brief meeting will be determined on the Pre-visit-teleconference call: ▪ Time, location and duration ▪ Attendees and contact information (e-mail, title, phone number, division)
	Schedule interviews with designated personnel ▪ Time, location and duration for each interview ▪ Contact information (e-mail, title, phone number, division) for each interview
	Schedule Daily Status meetings: ▪ Time, location and duration ▪ Contact information (e-mail, title, phone number, division)
	Scheduled Out-Brief meeting: ▪ Time, location and duration ▪ Attendees and contact information (e-mail, title, phone number, division)
	On-site Administrative Requirements:
	Parking permits, building access identifications and property passes.
	A secure area with 3 desks and 3 PCs and a printer with network connectivity to be used solely by CMS and [CONTRACTOR] personnel for testing and document review during the duration of the test. The PCs shall be configured with standard MS Office or equivalent software.
	Three (3) network connections including Internet access for [CONTRACTOR] and CMS laptops.
	Telephone access within the secured area for use by CMS and [CONTRACTOR] personnel
	If needed, a set of domain/network user Ids.

Attachment 2 –Sample Systems for Control Review

Server Name	IP address	Description

ATTACHMENT 3 –SCHEDULE

Timeframe and Schedule		
Day 1: Security Planning (SP)	**Day 2: Contingency Planning (CP)**	**Day 3: Configuration Management (CM), System Information Integrity (SI)**
In-Brief Meeting at 9 AM	If necessary, review CP documentation	If necessary, review CM documents
Participate in a walkthrough of the Data Center	Review and validate CP is consistent with documentation	Review and validate CM is consistent with documentation
If necessary, review SP documentation	Conduct CP interviews	Review logs for access attempts
Review and validate security policies	Daily status meeting	Review and validate Operating System configuration
Conduct SP interviews		Evaluate application configuration implementation
Daily status meeting		Review and validate sample system configuration and security controls
		Conduct CM interviews
		If necessary, review SI documents
		Review and validate SI process is consistent with documentation
		Review and validate: virus protection; flaw remediation; malicious code protection; intrusion detection tools and techniques; security alerts and advisories; and software information and integrity tools
		Conduct SI interviews
		Daily status meeting
Day 4: Audit and Accountability (AU), Risk Assessment (RA)	**Day 5:TBD**	**Additional Days: TBD (if needed)**
If necessary, review AU and RA documents	Provide overview of week's testing	TBD
Review and validate the AU and RA processes are consistent with documentation	Review "*Tentative*" findings	TBD
Conduct AU and RA interviews	Discuss next steps with expected due dates	TBD
Daily status meeting	Identify and document any action items	TBD
	Address any final questions	TBD

Note: This schedule may vary depending on work load.

ATTACHMENT 4– ON-SITE TECHNICAL STAFF AVAILABILITY REQUIREMENTS

Staff	Day 1 (mm/dd/yy)	Day 2 (mm/dd/yy)	Day 3 (mm/dd/yy)	Day 4 (mm/dd/yy)	Day 5 (mm/dd/yy)
System Security Officer (SSO)					
System Administrator					
Data Center Network Administrator					
Database Administrator					
Facility Manager					
Human Resources Manager					
Additional Users					

Note: Please check off the appropriate day for availability of technical staff.

APPENDIX D –TEST SCRIPT TEMPLATE

1. [CATEGORY (E.G., ACCESS CONTROLS)]

Function	Oversight Protocols	Requirements Met? Y / N / n/a	Work Paper References and Comments
[CATEGORY (E.G.,ACCESS CONTROLS)]			
e.g., AC-1. Policy and Procedures A formal, documented, policy that addresses purpose, scope, roles, responsibilities, and compliance must be developed, disseminated and periodically reviewed/updated.	1. Review the documented Policy. 2. Verify…… 3. Interview……. 4.		

DRAFT REQ

End of Document