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 Information Security Risk Assessment (RA) and System Security Plan (SSP) Guidance

Version 1.0
September 3, 2004

TABLE OF CONTENTS

1. INTRODUCTION

The Systems Security Group (SSG) of the Centers for Medicare & Medicaid Services (CMS) has developed this document to provide additional direction for the CMS Information Security Risk Assessment Methodology[1] and the CMS System Security Plan Methodology[2]. These methodology documents provide guidance for the proper development of Information Security Risk Assessments (IS RAs) and System Security Plans (SSPs). This document serves as a supplemental direction to the methodologies to assist authors with developing IS RAs and SSPs to expected CMS SSG standards. The guidance increases the clarity of the methodologies, as well as general structural and contextual improvements for IS RAs and SSPs.

The IS RA will be presented to the CMS CTO upon completion. The CTO will gain an understanding of the system, its business function, technologies to be implemented and risks introduced to the CMS business, and information resulting from the system's implementation.

2. BACKGROUND

As required by the Federal Information Security Management Act (FISMA), Federal agencies must develop, document, and implement an agency-wide information security program to protect information and information systems that contain sensitive information. The CMS SSG is meeting these requirements by using the National Institute of Standards and Technology (NIST) Special Publication 800-37 – *Guide for the Security Certification and Accreditation of Federal Information Systems* as the foundation for CMS' standards, policies and procedures. IS RA's and SSP are key components to the IT certification and accreditation process.

CMS has developed an information security program, which requires the development of IS RAs and SSPs for all information systems which store or process sensitive information. To ensure that IS RA and SSP documents are developed in an efficient and consistent manner, the CMS Information Security Risk Assessment Methodology and the CMS System Security Plan Methodology were developed. Although these documents provide guidance as to the proper development of IS RAs and SSPs, the CMS SSG has determined that additional guidance is needed. This document has been created, based upon a collaborative effort of members of the SSG, as to how IS RA and SSP documents shall be structured and developed.

3. WHICH DOCUMENTS REQUIRE A RISK ASSESSMENT AND SYSTEM SECURITY PLAN

The safe operation of systems which can store and process sensitive information is a requirement for all systems that operate within the CMS environment. To ensure the security of all General Support Systems (GSS), Major Applications (MA), and other critical system types, IS RAs and SSPs shall be developed in accordance with the guidelines established in the following table:

[1] Version 1.1, September 12, 2002

[2] Version 3.0, November 6, 2002

Table 1 System Types that require RA and SSP

System Type	IS RA	SSP
General Support System (GSS)	●	●
GSS or Major Application (MA) hosted outside the CMS Data Center	●	●
MA hosted on certified GSS	●	
Internet-facing System (GSS or MA)	●	●
All Pilots	●	●
"Other" System (At Chief Technology Officer's (CTO's) discretion)	●	●
System Family		
▪ MA covered by System Family	●	
▪ MA not covered by System Family	●	●

4. GENERAL GUIDANCE

This section addresses the general requirements for completing CMS IS RAs and SSPs. It provides guidance for developing IS RAs and SSPs in a manner consistent with the proper structure, content, and developmental steps.

4.1. STRUCTURE

The guidance provided in this section addresses the general structure of IS RA and SSP documents. Specific issues addressed by the SSG are as follows:

- Templates for IS RAs and SSPs are available from CMS' website. The address for this site is http://cms.hhs.gov/it/security/References/ps.asp

- Specific sections are shared between the IS RA and SSP documents. These sections correlate in the following manner:

Table 2 Section Mapping between IS RA & SSP

Section Title	IS RA	SSP
System Identification	1.1.1	1.1
System Organization	1.1.2	1.2
Information Contacts	1.1.3	1.3
Assignment of Security Responsibility	1.1.4	1.4
Document System Purpose and Description	1.2	1.6
System Environment and Special Considerations	1.2.1	1.6.1
System Interconnection/Information Sharing	1.2.2	1.6.2
System Security Level	1.3	1.6.4
Risk Determination Table Safeguard Determination Table	2 3	2.1†

[†] Vulnerabilities identified in the IS RA Section 2 – Risk Determination Table with moderate or high-risk levels shall be included in the SSP Section 2.1. Information from the IS RA Section 3- Safeguard Determination Table shall be included in SSP Section 2.1.

- Sections 1.2.1 and 1.2.2 for IS RAs may be further sub-divided in order to organize properly the information being presented. However, no additional numbering shall be used to represent the changes in organization. Use of bold and underline formatting are recommended to highlight these sub-divisions.

- Stated restrictions for the number of paragraphs are recommendations, and thus, are not a requirement for the proper development of IS RAs and SSPs.

- Figures and diagrams shall be labeled as "Figure 'X'" or "Diagram 'X'", with 'X' representing a numerical value based upon a sequential order of numbers. Individual components within each figure or diagram shall be identified by number, and referenced in the narrative by these numbers when describing component functions, information flow, etc.

- Supporting documentation shall not be attached, unless specifically requested by CMS officials.

- The number of references to other documents shall be minimized to simplify readability and information flow.

- IS RA and SSP documents are considered sensitive material and as such shall be marked at the bottom of each page, "CMS Sensitive Information/Requires Special Handling".

4.2. CONTENTS

The guidance provided in this section addresses the contents of the IS RA methodology and the SSP methodology documents. Specific issues addressed by the SSG are as follows:

- In both of the methodologies detailed descriptions are required that fully explain a system and its technical implementation to a level that can be understood by a reader who is unfamiliar with the system.

- Documents shall be written in present tense, describing the system as-is and shall include the in-place security controls for the version of the system referenced. Future enhancements or planned controls shall be mentioned only as recommended safeguards in the IS RAs Safeguard Determination Phase section and in the SSPs Risk Management section. If the system is newly developed and not yet in production, the IS RA and SSP must reflect the system and security controls that will be in place the day the system goes live.

- IS RA and SSP documents shall be written in a manner that will permit a reader unfamiliar with a system and its technical implementation to gain a thorough understanding of its purpose, operation, and technical details. Throughout the development process for IS RAs and SSPs, all security controls shall be described in detail. Technical information is relevant, yet the presentation must be clear and pertinent to the information being described. Explain/describe the terms specific to the implementation (may be related to the software/hardware used).

- Pertinent information describing how a control is implemented and how it addresses system security shall be included.

- Enough information shall be included in the IS RA and SSP. Reference to other supporting documents shall be made for detailed information.

- When referencing supporting or other available documentation, applicable content related to security controls shall be summarized. The document title, date, location, and contact information shall be provided. Contact information must include a person’s name, organization/office name, and phone number. Providing this information satisfies the IS RA and SSP document auditability requirements.

- The company name and function served for each contractor referenced in the IS RA and SSP shall be specifically identified.

4.3. DEVELOPMENT

The guidance provided in this section addresses the development of the IS RA and the SSP. Specific issues addressed by the SSG are as follows:

- Sections 1.2, 1.2.1, and 1.2.2 of the IS RA shall be finalized and approved by the SSG prior to moving forward with the development of the document. The proper completion of these sections is vital because they serve as the building blocks on which the rest of the IS RA and SSP are constructed.

- A skeleton SSP may be created for use during the development of an IS RA for systems which also require an SSP. The skeleton SSP may be used to record known controls identified during the IS RA authoring process. This could be accomplished by inserting placeholders in sections 2, 3, and 4 of the SSP for all controls, even though some controls will be explained in more detail or require additional information from other staff/components. This process should save time and ensure consistency of information between documents.

- The CMS Information Security Levels shall be used as a tool to identify the system security level. The rating dictates the level of security controls for the entire system. The system’s existing security controls and safeguards shall be documented based on the system’s information security level according to the CMS Acceptable Risk Safeguards (ARS) tool.

5. RISK ASSESSMENT METHODOLOGY

The CMS Information Security Risk Assessment Methodology details the steps required to ensure the proper development of IS RAs. In the process of completion of CMS IS RAs, specific issues arose which the SSG felt shall be addressed. Therefore, this guidance was created to ensure that IS RAs are developed in a consistent manner. Specific issues addressed by the SSG are as follows:

Section 1.1.3 – Information Contacts

- Internal applications within a system family SSP require the system owner to be the Group Director or above. Otherwise, the contact person must hold an office-level position, such as Office/Center Director, Vice President, etc.

- For systems housed/hosted outside of the CMS Data Center facilities, two system owners/managers are required; one for the CMS component overseeing the system's implementation and another for the contractor or external business partner hosting the system.

Section 1.1.4 – Assignment of Security Responsibility

- A CMS individual responsible for security and a component ISSO shall be identified for all systems. Additionally, corresponding emergency contacts shall be identified. A total of four different security contacts shall be provided.

- If a system is housed or hosted outside of the CMS Data Center facilities, an individual responsible for security and/or a component ISSO contact shall be provided for the contractor or external business partner hosting the system. Contractors or external business partners may have a designated Systems Security Officer that qualifies as the ISSO contact.

Section 1.2 – Document System Purpose and Description

- This section shall be titled *System Purpose and Description (Asset Identification)*.

- A high level description of the location of the system (external, internal) shall be provided. The description shall include the street address and other detailed location information.

- Describe the business function for each system.

- Describe each system's operation and information as a system asset.

- Describe the user community for the system and the users' level of access to the data (read, modify, etc).

- Develop a description for the business flow of the information. Describe how the data/information is handled by the system, including if the data is read, stored, purged, etc.

Section 1.2.1 – System Environment and Special Considerations

- This section shall provide a detailed description of the system's boundaries and technical components.

- Detailed hardware equipment information, such as server names, shall be listed and attached to the documentation (see Attachment 2).

- Include information concerning a system's hardware and platform(s).

- The system boundary and scope shall be identified.

- Describe the system architecture, the functional areas within the architecture (presentation, application and data zones, if applicable) and how this addresses security.

- For systems that interface with the Internet, describe how the architecture does/does not match the CMS Internet Platform Architecture. Identify every part of the system architecture that does not comply with the CMS Internet Platform Architecture as a risk in the Risk Determination Table. All planned safeguards for these risks shall be documented in the Safeguard Determination Table.

- Attach the network connectivity diagram, including the system components' connection, and the security devices which protect the system and which monitor access and system activity. For systems that have more than one server of the same type, include one in the diagram and state the accurate count of the servers in the text description. (Provide for opening sentence(s) prior to the diagram). After the diagram, include text explaining system components and function. System components in diagrams and text shall be numbered to correlate the information presented.

- Describe how system users access the system (i.e. desktop, thin client, etc.). Include any information required to evaluate the security of the access.

- Include a logical diagram for system components with system boundaries, if needed, to clarify understanding of the system function and integration.

- Following the logical diagram, describe the information flow or processes within the system to access to the data/information.

- Describe the connectivity between modules within the scope of this system. Connectivity with components/ systems outside of the scope of this system shall be included in section 1.2.2.

- Describe the information/data stores within the system and security controls for such data.

- Include the detailed implementation controls if system category is part of a system family not requiring a separate SSP.

Section 1.2.2 – System Interconnection/Information Sharing

- Include detailed descriptions of interconnections to other systems/applications outside the scope of the documented system. These interconnections shall be correlated to possible threats and vulnerabilities introduced by such connections and described in section 2.

- Include a network connectivity diagram to depict system interconnections. The diagram/figure presented in section 1.2.1 becomes the center cloud and part of the diagram/figure in section 1.2.2. Systems/ components shall be numbered for reference in text when describing the function and/or interconnections.

- Include a logical diagram, if needed, to clarify/present the information flow and interconnections.

- Describe the connectivity between systems.

- Describe the physical and logical security controls between systems.

- Describe the information/data that is shared and transmitted between systems, and the security controls that are implemented to safeguard confidentiality, integrity and availability such as encryption, VPNs, etc.

- Describe how information/data is accessed in other systems and what rights (“read”, “modify”, etc) the current system is granted on other interconnected system(s) and vice versa.

- Document the interconnection or information sharing agreements. If no agreements exist, state so, and include this as a risk in Section 2: Risk Determination.

- Include the detailed implementation controls if the system category is part of a system family not requiring a separate SSP.

Section 2 – Risk Determination Phase

- Threats and vulnerabilities shall be treated as a pair. Each threat/vulnerability pair shall be addressed individually to simplify identification of existing controls for the threat/vulnerability pair and for the determination of the risk level. If multiple vulnerabilities are matched to a single threat, existing controls may not be applicable to all vulnerabilities identified.

- Evaluate the resulting risk level based upon a specific vulnerability instead of an overall correlation of multiple vulnerabilities.

- Address threats and vulnerabilities introduced by system users and system administrators, and the administration method/access (local, remote).

- Document the existing controls.

- If a penetration test has been conducted for the system, include threats and vulnerabilities identified in the penetration test report, including possible unauthorized access to the system, configuration vulnerabilities and other existing controls or vulnerabilities, as appropriate.

- The Risk Determination Table shall meet the following requirements:
  - The table may be changed to landscape orientation to facilitate readability and to allow more detailed information in control description.
  - The item numbers shall be sequential. Include system acronym in front of the number for traceability. Ex: EDB-1.
  - Threat/vulnerability pairs may be grouped by category (environmental/physical, human, natural and technical) for clarity. Other categories may be created as necessary during the risk assessment analysis.
  - Vulnerabilities must address system weaknesses that could be exploited by the threat(s).
  - The risk description shall be tailored to the system and shall be described in terms of confidentiality, integrity and availability of data, systems, and the business functions. Do not copy the description included in the CMS Threat Identification Resource.
  - Existing controls shall be grouped by type (management, operational, technical). Existing controls listed/described shall be consistent with the information presented in the SSPs sections 2, 3 and 4.

Section 3 – Safeguard Determination Phase

- Recommended safeguards shall completely address the threat/vulnerability pair identified as high- or moderate-level risk in corresponding items in the Risk Determination Table (Section 2).

6. SYSTEM SECURITY PLAN METHODOLOGY

The CMS System Security Plan Methodology provides detailed instructions defining the steps required for the proper development of SSPs. In the process of completion of CMS SSPs, specific issues arose which the SSG determined shall be addressed. Specific issues addressed by the SSG are as follows:

Section 1 – System Identification

- Use Section 1 from the IS RA and add sections not developed for IS RA.

Sections 2, 3, 4 – Management Controls, Operational Controls, Technical Controls

- Management, Operational and Technical Controls sections shall address and expand upon existing security controls listed in the Risk Determination Table of the IS RA.

Section 2.1 – Risk Assessment and Risk Management

- Include items with moderate and high-risk levels as identified on section 2 of IS RA, as follows (See Attachment 1):
  - IS RA, Risk Determination table, column titled 'Vulnerability Name' corresponds to SSP, Section 2.1 table, column titled 'Vulnerability'.
  - IS RA, Risk Determination table, column titled 'Risk Level' corresponds to SSP, Section 2.1 table, column titled 'Risk Level'.
  - Recommended Safeguard Determination table of the IS RA, column titled 'Recommended Safeguard Description' corresponds to SSP Section 2.1 table, column titled 'Recommended Safeguard'.
  - Recommended Safeguard Determination table of the IS RA, column 'Residual Risk Level' corresponds to SSP Section 2.1 table, column titled 'Residual Risk'.
  - Column titled 'Status of Safeguard' of the SSP Risk Assessment and Risk Management table in Section 2.1 describes the implementation status of recommended safeguard.
  - Column titled 'Updated Risk' of the SSP Risk Assessment and Risk Management table in Section 2.1 describes risk level based on the implementation status of the recommended safeguard. If the recommended safeguard is not fully implemented and any implementation to date changes the risk level for the evaluated threat/ vulnerability pair, the Updated Risk shall be changed accordingly.

Section 2.3 – Rules of Behavior, Section 3.1 – Personnel Security Controls

- CMS shall address security controls and inherited risk from system users and the system administrator. If the system user is outside the system maintainer's purview, information shall be included from the system/business owner's perspective.

Section 3.1 – Personnel Security Controls

- Include the description of background checks for employees and applicable security clearances.

Section 3.2 – Physical and Environmental Protection Controls

- Describe secure spaces/areas, such as server rooms, etc.

- Describe the physical controls that have been implemented, such as guard services, card key access, etc.

Section 3.4 – Incident Response Capability

- Describe the correlation of suspicious activity/events across various security/monitoring devices, such as IDS, firewall/router logs, etc.

- Describe how the vulnerabilities are identified, tracked, and resolved.

Section 3.5 – Contingency Planning and Disaster Recovery Planning

- Describe the testing of recovery procedures, how often they are performed, who is to perform the testing and where the results of the testing are stored.

Section 3.6.2 – Environmental System Software Management

- Describe patch management procedures.

Section 3.7 – Data Integrity/Validation Controls

- List the anti-virus software that is used and on which system components it is implemented. Also, describe how often signatures are updated and how notification of signature update availability is conducted.

- Describe the validation routines, if applicable.

Section 4.1 – Identification and Authentication Controls

- Describe any two-factor authentication methods that are used.

Section 4.3 – Remote Users and Dial-up Controls

- Describe the access controls implemented for system users and system administrators.

Section 4.4 – Wide Area Networks (WAN) Controls

- Describe the implementation of firewalls, routers/ switches, VPNs, etc. Include any MDCN components implemented as perimeter protection, but do not describe MDCN security controls, since it may be out of the system's scope, unless the system's components are an integral part of the MDCN.

- Describe the administration of security devices, such as remote/local console and security controls to protect such access: two-factor authentication, encryption, etc.

7. TOOLS

This section identifies tools which shall be used in conjunction with the creation of RAs and SSPs for CMS. Listed are combinations of tools, both CMS-owned and publicly available, for use by individuals responsible for the creation of CMS IS RA and SSP documents.

Risk Assessment and System Security Plan Tools			
Item #	**Tool**	**Location**	**Remarks**
1.	CMS Information Security Risk Assessment Methodology	http://cms.hhs.gov/it/security/docs/RA_meth.pdf	• None
2.	CMS Information Security Levels	http://cms.hhs.gov/it/security/docs/ssl.pdf	• Use this tool for the completion of Section 1.3 of the IS RA. • Use only one security level for the system in the table, but many information categories can be described in text of Section 1.3.

Risk Assessment and System Security Plan Tools			
Item #	**Tool**	**Location**	**Remarks**
3.	CMS Threat Identification Resource	http://cms.hhs.gov/it/security/docs/Threat_ID_resource.pdf	• This tool shall be used as a baseline. Not all threats are applicable to all systems. • Address general Personnel Security and Rules of Behavior in appropriate sections (if system category is part of a system family not requiring a separate SSP). • This tool can be used in the identification of further threats, depending on the system environment and interconnections.
4.	CMS System Security Plan Methodology – Appendix A Template	http://cms.hhs.gov/it/security/docs/ssp_meth.pdf	• Use the security controls categories in the Management, Operational and Technical Controls sections as a guide for existing security controls for the development of the Risk Determination Table.
5.	CMS Acceptable Risk Safeguard	http://cms.hhs.gov/it/security/docs/ars.pdf	• Use this tool as a standard for minimum-security controls expected for internal CMS systems.
6.	CMS Information Security Terms and Definitions	http://cms.hhs.gov/it/security/docs/termsanddefinitions.pdf	• None
7.	CMS Information Security Acronyms	http://cms.hhs.gov/it/security/docs/acronyms.pdf	• None
8.	Penetration Testing Report	Not Available	• None
9.	CMS Internet Architecture, July 2003	http://cms.hhs.gov/it/enterprisearchitecture/internetarch.pdf	• None
10.	Core Set of Security Requirements for External Business Partners	http://cms.hhs.gov/manuals/117_systems_security/117_systems_security_atcha.pdf	• Refer to Contractor Assessment Security Tool (CAST).

Risk Assessment and System Security Plan Tools			
Item #	**Tool**	**Location**	**Remarks**
11.	Contractor Assessment Security Tool (CAST)	http://cms.hhs.gov/it/security/docs/cast.zip	• This tool shall be used for security controls categories, as required by CMS and other Federal regulations (HIPAA, FISCAM, IRS, etc).
12.	NIST Special Publication 800-6, Security Self-Assessment for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf	• None

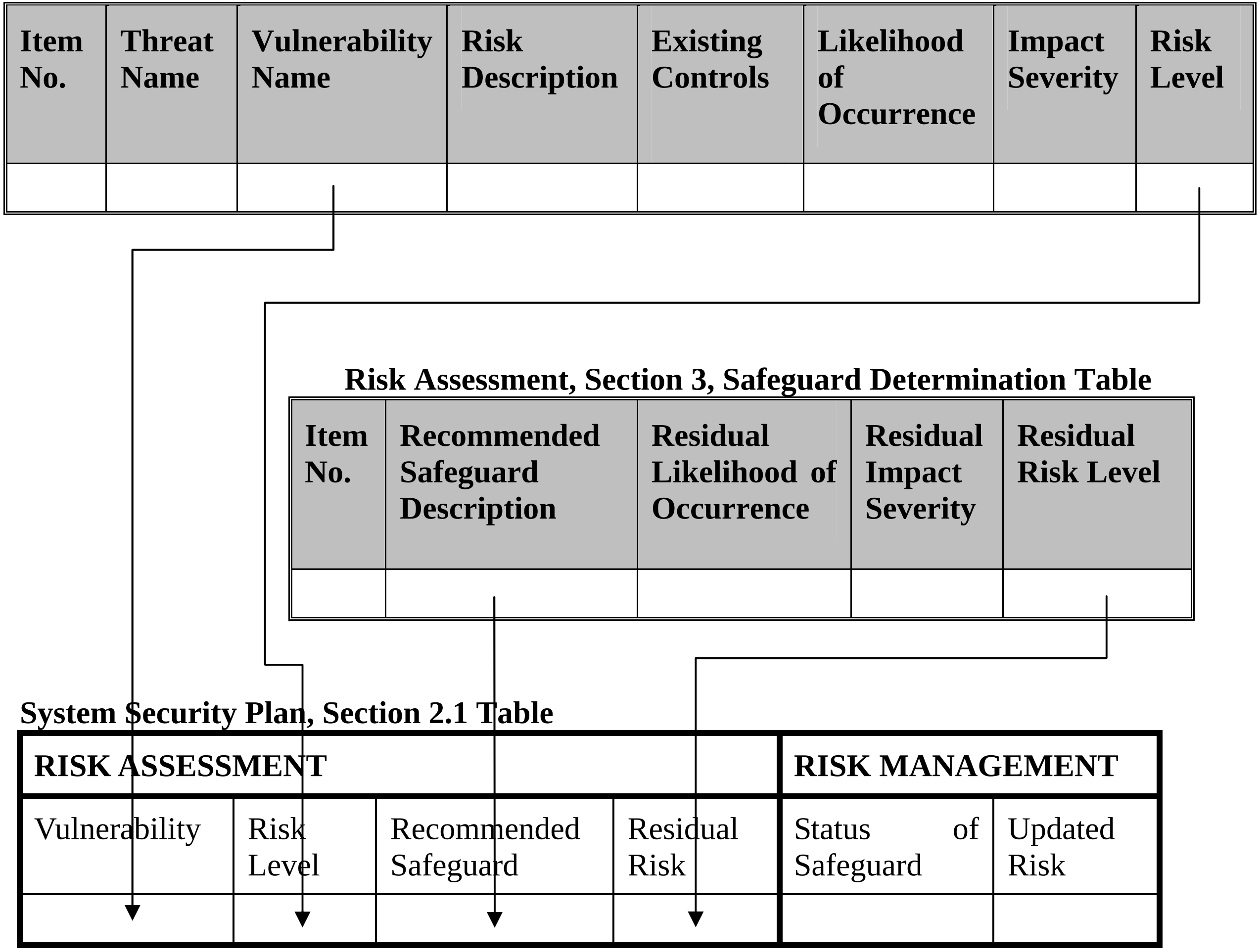
8. LINKS

The following are identified links that may be used to reference identified tools and other relevant materials required for the completion of the IS RA and SSP documents for CMS. Links have been included to obtain this data for locations both internal and external of the CMS network. The links are as follows:

External: http://cms.hhs.gov/it/security/References/ps.asp

Internal: http://cmsnet.cms.hhs.gov/cybertyger/

ATTACHMENT 1



Risk Assessment, Section 2, Risk Determination Table

Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level

Risk Assessment, Section 3, Safeguard Determination Table

Item No.	Recommended Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level

System Security Plan, Section 2.1 Table

RISK ASSESSMENT				RISK MANAGEMENT	
Vulnerability	Risk Level	Recommended Safeguard	Residual Risk	Status of Safeguard	Updated Risk

ATTACHMENT 2

Hardware Listing Table

Hardware Component (Server, router, firewall, etc name – same as Diagram)	**System Function**	**Server Type** (Make, Model, etc)	**Operating System** (Version, **Patch level, etc)**	**Software** (name, Vendor, version)	**Qty.** (No. of Servers)

End of Document