Risk Assessment Report (RAR)

<Company Name>

<System Name>

<Date>

TABLE OF CONTENTS

TABLE OF TABLES

1. Introduction

The Risk Assessment Report (RAR) documents the results of planning and implementing adequate, cost-effective security protection for a system. It reflects input from management responsible for the system, including the system owner, information owners, the system operator, the system security manager, and system administrators.

The purpose of the RAR is to provide an overview of the security of the information system and to describe the controls and critical elements in place or planned for, based on a vulnerability assessment to the threats to the organization. This RAR follows guidance consistent with the concepts presented in the National Institute of Standards and Technology Special Publications (NIST SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

This Risk Assessment Report (RAR) was developed by Your Cybersecurity Matters under the direction of the <specify IC manager for whom the work was performed>. This RAR is based upon a review of the environment, documentation, NIST regulations/guidance, and interviews with the information system personnel. In addition to this report, a System Security Plan (SSP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M) have been developed under this effort. The RAR documents the risk assessment approach used to determine the overall risk posture of the system, and it addresses security concerns that may affect the system.

1.1 System Description

<System Name>			
<Company Name> Prepared this Assessment			
	Confidentiality Value (Low, Moderate, High)	Integrity Value (Low, Moderate, High)	Availability Value (Low, Moderate, High)
System Categorization (from SSP, Section 2.1)	Moderate	Moderate	Moderate

1.2 Scope

The scope of this risk assessment is focused on the organization use of resources and controls to mitigate vulnerabilities exploitable by threat agents (internal and external) identified during the RMF control assessment process based on the system's categorization, which by definition is rated as moderate.

This initial assessment will be a Tier 3 or "information system level" risk assessment. While not entirely comprehensive of all threats and vulnerabilities to <System Name>, this assessment will include any known risks related to the incomplete or inadequate implementation of the NIST SP 800-171 controls selected for this system. This document should be updated annually as vulnerabilities to threats are mitigated through POA&M action.