System Security Plan (SSP)

<Company Name>

<System Name>

<Date>

TABLE OF CONTENTS

Executive Summary

Companies that provide employees to the Federal Government are required to identify each information system that contains, processes, and transmits Controlled Unclassified Information (CUI) and to prepare and implement a plan for the security and privacy of these systems. The objective of system security planning is to improve protection of information technology (IT) resources. All information systems have some level of sensitivity and require protection as part of best-management practices. The protection of a system must be documented in a System Security Plan (SSP).

The SSP is viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It reflects input from management responsible for the system, including information owners, the system operator, the system security manager, and system administrators. The SSP delineates responsibilities and expected behavior of all individuals who access the system.

The purpose of this SSP is to provide an overview of the security of the <System Name> and describe the controls and critical elements in place or planned for, based on NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*. Each applicable security control has been identified as either in place or planned. This SSP follows guidance contained in NIST Special Publication (SP) 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems, February 2006.*

This System Security Plan (SSP) provides an overview of the security requirements for <System Name> and describes the controls in place or planned for implementation to provide a level of security appropriate for the information processed as of the date indicated in the approval page.

Note: The SSP is a living document that will be updated periodically to incorporate new and/or modified security controls. The plan will be revised as the changes occur to the system, the data, or the technical environment in which the system operates.