# Hi I am an H1

## Hi I am an H2

1. FIRST ITEM
2. SECOND ITEM

* ONE
* TWO

TITLE

**SYSTEM SECURITY PLAN (SSP)**

**National Reconnaissance Office**

Project ID: **200410**

Project Name: **Unclassified Enterprise Continuous Monitoring**

Date: **08-23-2021**

<

***Introduction***

*(U//FOUO) The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources and Public Law 107-347, the Federal Information Security Management Act (FISMA), NIST Special Publication 800-37 Rev.  2, Guide for Applying the Risk Management Framework to Federal Information Systems, and Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253, Security Categorization and Control Selection for National Security Systems. Federal agencies are required to identify each computer system that contains sensitive information, 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.  The protection of a system is documented in a System Security Plan (SSP).*   
*(U//FOUO) The SSP 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 information system owner, 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.*

*(U//FOUO) The purpose of the SSP 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 CNSS Instruction 1253.  The SSP provides sufficient information to enable an understanding of the implementation of each security control in the context of the information system.  The System Security Plan also contains as supporting appendices or as references to appropriate sources, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.  This SSP template follows guidance contained in NIST Special Publication 800-37 Revision 2.*

<

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **User** | **Role** | **Employee Type** | **Email** |
| ISO Test | ISO |  | Joshua.hill@recro.com |
| Joshua Hill | ISO |  | joshua.hill@recro.com |
| Taylor Wirth | ISO | GOV | taylor.wirth@recro.com |