01 SYSTEM IDENTIFICATION

System identification in the System Security Plan (SSP) creates a detailed inventory of the system, its components, purpose, and connections. This helps organizations understand the scope of their security responsibilities, assess risks, and implement appropriate security controls to protect sensitive data. ref. 01 System Identification

01.01 System Name (title): The "System Name/Title" in a System Security Plan (SSP) is a concise and descriptive name that uniquely identifies the information system or system component covered by the plan. It should be easily recognizable and understood by stakeholders, enabling clear communication and reference throughout the SSP document.

[State the name of the system. Spell out acronyms.]

01.01.01 System Categorization: (System categorization in an SSP is the process of classifying your information system based on the potential impact (low, moderate, or high) that the loss of confidentiality, integrity, or availability of the information it processes would have on your organization. This categorization drives the selection of appropriate security controls to protect the system and its data.)

[low impact, moderate impact, high impact]

01.01.02 System Unique Identifier: (The System Unique Identifier in a System Security Plan is a designated value, like a name or serial number, that distinctly identifies the specific system being documented. This identifier helps differentiate the system from others and ensures clarity when referencing it in security assessments, audits, or other documentation.)

[Insert the System Unique Identifier]

01.02 Responsible Organization: The "Responsible Organization" in a System Security Plan (SSP) is the entity that owns and operates the information system and is ultimately accountable for the security of the system and the Controlled Unclassified Information (CUI) it processes, stores, or transmits. This organization is responsible for implementing and maintaining the security controls outlined in the SSP and ensuring compliance with NIST SP 800-171 Rev. 3.

Name:	[company name]
Address:	[company address]
Phone:	[company phone number]

01.03 Responsible Positions within the Organization

Defining specific responsibilities for overseeing the System Security Plan (SSP) is essential for ensuring accountability, promoting ownership, and facilitating effective management. Clear roles ensure the SSP is actively maintained, updated, and used to guide security practices. This clarity streamlines communication, supports compliance. These individuals need to comply with an established company policy. ie. Example of a Personnel Vetting Policy for ITAR

01.03.01 Information Owner: The Information Owner in a System Security Plan is the official responsible for the CUI. They have the authority to determine the information's classification, how it's used, and who can access it. They set the rules for protecting the data and ensure proper security controls are in place. (ie. the owner or CEO)

Name:	[name]
Title:	[title]
Address:	[company address]
Phone:	[company phone number]
Email Address:	[company email address]

01.03.02 System Owner: The System Owner in a System Security Plan (SSP) is the person or group responsible for the system's entire lifecycle. This includes its training, financial support, development, operation, maintenance, and eventual disposal. They ensure the system meets security requirements and aligns with organizational goals. (ie. the the person acting as COO, CFO or CIO)

Name:	[name]
Title:	[title]
Address:	[company address]
Phone:	[company phone number]
Email Address:	[company email address]

01.03.03 System Security Officer: The System Security Officer (SSO) is the individual responsible for the system's security posture. They implement and maintain security controls, ensure compliance with all directed security measures, and manage ongoing security assessments and risk mitigation.

Name:	[name]
Title:	[title]
Address:	[company address]
Phone:	[company phone number]
Email Address:	[company email address]

01.04 General Description (purpose of system): What is the function/purpose of the system?

[Provide a short, high-level description of the function/purpose of the system.]

01.05 General Description of Information: CUI information types processed, stored, or transmitted by the system are determined and documented. For more information, see the CUI Registry at https://www.archives.gov/cui/registry/category-list.

[Document the CUI information types processed, stored, or transmitted by the system below]

02 SYSTEM ENVIRONMENT

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note: this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram. ref. 02 System Environment

[Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]

02.01 List all Hardware and Person or Role Responsible

[Worksheet for List all Hardware and Person or Role Responsible]

02.02 List all Software Components Installed on the System and Person or Role Responsible

[Worksheet for List all Software Components Installed on the System and Person or Role Responsible]

02.03 Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization?

[Yes/No - If no, explain:]

03 REQUIREMENTS

(Note: The source of the requirements is NIST Special Publication 800-171 Revision 3, dated May 14, 2024)

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

See Section 3.0 Requirements Worksheet for specific details

04 RECORD OF CHANGES

The "Record of Changes" within a system security plan is a critical log that documents all modifications made to a system. It ensures accountability by tracking who made changes, when, and why, providing a historical record of the system's evolution. This record supports audits, aids in troubleshooting and incident response, and facilitates rollback if needed. By maintaining a detailed record of changes, organizations demonstrate compliance with security standards like NIST 800-171 and ensure the ongoing security and integrity of their systems. ref. 04 Record of Changes

[Worksheet for Record of Changes]