1. **SYSTEM IDENTIFICATION**
   1. **System Name/Title: {iATMName}**
      1. **System Categorization: Moderate Impact for Confidentiality**
      2. **System Unique Identifier: {iATMId}**
   2. **Responsible Organization:**

|  |  |
| --- | --- |
| Name: | {vOrganizationName} |
| Address: | {vOrganizationAddress} |
| Phone: | {vOrganizationPhone} |

* + 1. **Information Owner (**Government point of contact responsible for providing and/or receiving CUI)**:**

|  |  |
| --- | --- |
| Name: |  |
| Title: |  |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

* + - 1. **System Owner** (assignment of security responsibility)**:**

|  |  |
| --- | --- |
| Name: | {iCertifyingUserName} |
| Title: | {iCertifyingUserTitle} |
| Office Address: | {iCertifyingUserAddress} |
| Work Phone: | {iCertifyingUserPhone} |
| e-Mail Address: | {iCertifyingUserEmail} |

* + - 1. **System Security Officer:**

|  |  |
| --- | --- |
| Name: | {iCertifyingUserName} |
| Title: | {iCertifyingUserTitle} |
| Office Address: | {iCertifyingUserAddress} |
| Work Phone: | {iCertifyingUserPhone} |
| e-Mail Address: | {iCertifyingUserEmail} |

* 1. **General Description/Purpose of System:**  What is the function/purpose of the system? **{vAssessmentDescription}**
     1. Number of end users and privileged users: **[In the table below, provide the *approximate* number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]**

**Roles of Users and Number of Each Type:**

|  |  |
| --- | --- |
| **Number of Users** | **Number of Administrators/**  **Privileged Users** |
|  |  |

* 1. **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**].

1. **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.

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

* 1. Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. **[Insert the reference/URL or note that the hardware component inventory is attached.]**
  2. List all software components installed on the system. **[Insert the reference/URL or note that the software component inventory is attached.]**
  3. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **[Yes/No - If no, explain:]**

1. **REQUIREMENTS**

**(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)**

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.

**{#checklist}**

**{#parent}**

**{ShortDescription}**

**{#child}**

**{ChecklistItemName}:** {LongDescription}

**Status: {ChecklistRecordStatus}**

**Results: {Results}**

**{/child}**

**{/parent}**

**{/checklist}**

1. **RECORD OF CHANGES**

|  |  |  |
| --- | --- | --- |
| **Date** | **Description** | **Made By:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

APPENDIX

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Deficiency** | **Res****ponsible** | **Resource**  **Estimate**  **(funded/ unfunded/ reallocation)** | **Milestone** | **Target Completion Dates** | **Actions** | **Status** ***(Ongoing or Complete)*** |
| **{#pmr}{Deficiency}** | {Responsible} | {ResourceStatus} | {MilestoneName} | {TargetCompletion} | {ActionNote} | {POAStatus}{/pmr} |