

**JSIG (53Rev4)**

**System Security Plan (SSP)**

|  |  |
| --- | --- |
| **Company/Organization Name** | <Organization> |
| **Location (City/State)** | <Location> |
| **System Name** | <Official System Name as listed on your Census> |
| **Registration # / Unique ID** | <System UID> |
| **System Classification//Caveats** | Secret//XXX <or Top Secret//XXX><Add all PIDs the system will process and SCI caveats if applies.> |
| **Security Categorization** | MML <System Categorization> |
| **Sponsoring Service/Agency**  | Air Force |

|  |  |
| --- | --- |
| **Version** | <Version> |
| **Date** | <Date> |

<Highlighted areas are either or completion or for notes/comments to the author. Please remove all highlights and notes when completing your SSP for submission.>

 **SYSTEM/DOCUMENT Change RECORDS**

*<The system changes provided within this table must be incorporated into the security plan annually, as a minimum; as system modifications require changes; and/or during system re-authorization. [PL-2]>*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SSP Revision Number | Description of change | Changed Page(s) | Date  | Entered BY |
| 1.0 | initial | n/a | date | your name |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Verification of Controls**

The signatories below attest that this System Security Plan (SSP) accurately reflects the security environment of the organization and system indicated below:

**ISO/PM GSSO/CPSO**

 **<Enter Name> <Enter Name>**

**ISSM ISSO**

 **<Enter Name> <Enter Name>**

**SA DTA**

 **<Enter Name> <Enter Name>**

<Enter all SAs and DTAs that participated in the creation of system BoE. If not, just list them in the Key Roles section.>

**TABLE OF CONTENTS**

Table of Contents

[1 SYSTEM IDENTIFICATION 6](#_Toc78288897)

[1.1 System Overview 6](#_Toc78288898)

[1.2 Security Categorization 7](#_Toc78288899)

[1.2.1 Control Selection 7](#_Toc78288900)

[2 KEY ROLES AND CONTACT INFO 8](#_Toc78288901)

[3 SYSTEM ENVIRONMENT 11](#_Toc78288902)

[3.1 Physical Environment 11](#_Toc78288903)

[3.2 Facility/System Layout 12](#_Toc78288904)

[3.3 Personnel Authorizations 12](#_Toc78288905)

[3.4 Account Management Policies 12](#_Toc78288906)

[4 GENERAL SYSTEM DESCRIPTION/PURPOSE 13](#_Toc78288907)

[4.1 System/Network and Functional Architecture 14](#_Toc78288908)

[4.2 User Roles and Access Privileges 17](#_Toc78288909)

[4.3 User-Developed Software 18](#_Toc78288910)

[5 INTERCONNECTIONS/INFORMATION SHARING 19](#_Toc78288911)

[5.1 Direct Network Connections 19](#_Toc78288912)

[5.2 Indirect Connections 19](#_Toc78288913)

[5.3 Memorandums and Agreements 20](#_Toc78288914)

[Appendix A: Acronyms 22](#_Toc78288915)

[Appendix B: System/network diagram 23](#_Toc78288916)

[Appendix C: Assured File Transfer Procedures 26](#_Toc78288917)

[Appendix D: SECURITY CONTROL TRACEABILITY MATRIX 27](#_Toc78288918)

[Appendix E: HARDWARE LIST 28](#_Toc78288919)

[Appendix F: SOFTWARE LIST 29](#_Toc78288920)

[Appendix G: User AgreementS 30](#_Toc78288921)

[Appendix H: NETWORK PORTS LISTING 31](#_Toc78288922)

<Add any other Appendices for ConOps, Dormant Hard Drive Procedures, Periods Processing Procedures, Virtualization Configuration Details, Multifactor Authorization Process, or other documentation. If Network Ports Listing is not used (e.g., standalone system), remove the Appendix*.>*

# SYSTEM IDENTIFICATION

## System Overview

**System Name:** <System Name (Same as listed on title page).>

**Unique Identifier:**  <System UID>

**System Operation Status:** Operational/Deployable. ATO Expiration 27 Jul 23.

<Insert the operational status of the system, e.g. in development, operational - undergoing modifications, deployed, etc. If deployable, see sample in Section 4.1 regarding deployable systems. Show ATO expiration date if operational.>

**System Type*:*** < AFTC System Types: Standalone (SA), Point-2-Point (P2P), or Collaborative Enclave (CE). If a single workstation, the system type would be Standalone (SA) Workstation. If an isolated network (no connections), the system would type would be Standalone (SA) Network. If directly connected to another network, the system type would be CE with Connection to NetworkName. See definitions below:

Standalones (SA): SA system/enclave is a single system or collection of systems that have no network connectivity other than to themselves. The systems/enclaves are all physically, not logically connected and wholly contained within the facility (i.e. same room, same lab, same building or adjacent building). The definition of a SA system is a closed-loop system/enclave with no persistent external connections. Internal connections include but not limited to optical media, approved external USB hard drives, and isolated switches connecting all nodes.

Point-to-Point (P2P): P2P systems are isolated, closed-loop systems or enclaves that intermittently connect one-to-one to other approved systems via a tunneling mechanism (e.g. TACLANE) and have no other external connections, except for the approved transport mechanism. The P2P systems are isolated with limited connectivity, i.e., completely closed until connected to another P2P using an approved transport mechanism. An MOA/MOU/ISA is required, along with details about the interconnection such as security controls or protections in place.

Collaborative Enclaves (CE): CE systems are more complex enclaves performing AFTC mission related functions. The CE system are usually connected to multiple domains at the same time and bring test components to evaluate. CE systems have persistent network connections and may be connected to other services or SAP networks.>

**System Classification and Programs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification** | **Formal Caveats** (PID/Trigraph(s)) | **Dissemination** (NOFORN, HVSACO) | **CSA** (Navy, AF…) |
| Secret | <PIDs> | HVSACO | AF |

<If periods-processing down to collateral, put “Up to Secret” in the Classification block. Ensure the ISO is fully aware and can validate the PIDs being on the system. This section is especially critical when identifying direct connections to other SAP systems for avoiding the high to low scenario. PM/ISO is responsible for the PID selection and it must match with any direct connections.>

##  Security Categorization

<For all systems, a Categorization Memo must be completed and sent to the AFTC AO for approval. The below information will be obtained from your approved Categorization Checklist.>

|  |
| --- |
| **System Impact Categorization** |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** | **Authority** |
| <Moderate> | <Low> | <Low> | AO |

For categorization selection justification, see system Categorization and Selection Checklist for L-XXXXX.

### Control Selection

|  |  |
| --- | --- |
| JSIG Reference: | 2.3.2  |

<Following ISO and SCA discussions on control selection, identify the applicable baseline and overlays, i.e., fill in the appropriate baseline and check applicable boxes.>

|  |
| --- |
| **Baseline**:  |
|  <MML or other approved categorization> |
| **Overlays** (Select/Add all that apply): |
|  | Accessibility (not all users are formally accessed to all data/programs) |
|  | CDS \_\_\_\_\_\_\_\_\_\_\_ Identify column used: Access, Transfer, or Multi-level  |
| X | Classified (This overlay applies to all SAP systems unless instructed otherwise by AO/SCA.) |
|  | Intelligence Overlay: \_\_\_\_\_\_\_\_\_\_\_ Identify column used: A, B, or C  |
|  | PII or Privacy |
|  | Standalone \_\_\_\_\_\_\_\_\_\_(Identify column used: Single User; Multiple Users; or Antivirus) |
|  | <Identify any other overlays used. If using PII overlay, attach the Privacy Impact Assessment.> |

# KEY ROLES AND CONTACT INFO

*<Tailor titles/key roles specific to your organization.>*

**Authorizing Official (AO)**

1. Name: Eileen A. Bjorkman
2. Organization: AFTC/CA
3. Address: 1 S. Rosamond Blvd, Edwards AFB CA 93524
4. Phone: 661-277-4366 (DSN 525)
5. Email: Eileen.bjorkman.1@us.af.mil

**Security Control Assessor (SCA)**

1. Name: Jesus Flores
2. Organization: 412 TW/IPIM
3. Address: 195 E. Popson Ave, Edwards AFB CA 93524
4. Phone: 661-277-8193 (DSN 527)
5. Email: jesus.flores.17@us.af.mil

**Security Control Assessor (SCAR)**

1. Name: William D. Donehue
2. Organization: 96 TW/AP (AFTC)
3. Address: 101 West D Ave Ste 250, Eglin AFB, FL 32542
4. Phone: 850-882-5643 (DSN 872)
5. Email: william.donehue.4.ctr@us.af.mil

**Information System Owner (ISO)/Program Manager (PM)**

1. Name: <Enter name>
2. Organization: <Enter organization>
3. Address: <Enter address>
4. Phone: <Enter phone #>
5. Email: <Enter email address>

**Program Security Officer/Manager (PSO/M)**

1. Name: Angela Myers
2. Organization: AFOSI/PJ Det 3
3. Address: 101 West D Ave Ste 250, Eglin AFB, FL 32542
4. Phone: 850-882-5828
5. Email angela.myers.1@us.af.mil

**Government/Contractor Program Security Officer (GSSO/CPSO)**

1. Name: <Enter name>
2. Organization: <Enter organization>
3. Address: <Enter address>
4. Phone: <Enter phone #>
5. Email <Enter email address>

**Information System Security Manager (ISSM)**

1. Name: <Enter name>
2. Organization: <Enter organization>
3. Address: <Enter address>
4. Phone: <Enter phone #>
5. Email <Enter email address>
6. 8570 Profile <Enter Profile, i.e. IAT/IAM Level>
7. 8570 Baseline Certification <Enter Baseline Certification>

**Information System Security Officer (ISSO)**

1. Name: <Enter name>
2. Organization: <Enter organization>
3. Address: <Enter address>
4. Phone: <Enter phone #>
5. Email <Enter email address>
6. 8570 Profile <Enter Profile, i.e. IAT/IAM Level >
7. 8570 Baseline Certification <Enter Baseline Certification>

**System Administrator/Network Administrator**

<Repeat contact info for each SA/NA or attach SA/NA listing with contact info.>

1. Name: <Enter name>
2. Organization: <Enter organization>
3. Address: <Enter address>
4. Phone: <Enter phone #>
5. Email: <Enter email address>
6. 8570 Profile <Enter Profile, i.e. IAT/IAM Level >
7. 8570 Baseline Certification <Enter Baseline Certification>
8. 8570 Computing Environment <Enter Computing Environment Certification>

**Data Transfer Agent (DTA)**

<Repeat contact info for each DTA or attach DTA listing with contact info.>

1. Name: <Enter name>
2. Organization: <Enter organization>
3. Phone: <Enter phone #>
4. Email: <Enter email address>

# SYSTEM ENVIRONMENT

## Physical Environment

|  |  |
| --- | --- |
| JSIG Reference: | PE-3 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Building Number:** | <Bldg> | **Room Number(s):** | <Room Number(s). Each room must have their own entry filled out.> |

|  |  |
| --- | --- |
| **Is the secure facility accredited or approved to process and store information at the level covered by this SSP?** | [ ]  Yes[ ]  No |
| **Who accredited or approved the facility?** | Organization: AFOSI/PJ Det X Name: <Accreditor> |
| **Indicate if the facility is a SAPF, SCIF, or Other.** | [x]  SAPF Date of Approval \_\_<Date>\_\_\_\_\_\_\_[ ]  SCIF Date of Approval \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[ ]  Other Date of Approval \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **State the highest classification level and programs/compartments approved for the facility.** | [ ]  Secret[ ]  Top Secret | [ ]  SAR[ ]  SCI | Others[ ]  \_\_\_\_\_\_\_[ ]  \_\_\_\_\_\_\_ |
| **Is the system approved for unattended processing?** | [ ]  Yes <Suggest you consider this one carefully in case you[ ]  No need to let things process after duty hours.> |
| **Is the facility approved for 24-hour operation?** | [ ]  Yes[ ]  No <Refer to Fixed Facility Checklist> |
| **Is the facility approved for Open or Closed storage?** | [ ]  Open [ ]  Closed [ ]  Modified Open Storage<Refer to Fixed Facility Checklist> |
| **List all items approved for Open Storage** | e.g. Hard drives, CD/DVDs, tapes, printouts, etc.<Refer to Fixed Facility Checklist> |
| **List all items restricted to Closed Storage** | e.g. Hard drives, CD/DVDs, tapes, printouts, etc.<Refer to Fixed Facility Checklist> |
| **[ ] All classified and unclassified systems co-located with this IS are identified in the box to the right.** **[ ]  No other systems are co-located with this IS.** <Make sure this section matches your Facility/System diagram.> | [ ]  NIPRNet/NMCI [ ]  Internet/Corporate LAN[ ]  SIPRNet[ ]  JWICSOther external IS[x]  CV2[ ]  <Name of System> | UnclassifiedUnclassifiedSecretSCIS//SAP<Classification Level> |

## Facility/System Layout

<Include or reference facility layout showing placement of physical devices, i.e., building floor plan depicting room(s) identified as SAPF with placement of system devices, e.g., servers, workstations, printers, scanners, etc. This is the room/facility layout and not the topology diagram (data flow). Having a legend and color coding the systems will help show the layout. Be sure to classify the layout diagram appropriately. >

<Sample Facility/System Layout>



## Personnel Authorizations

|  |  |
| --- | --- |
| JSIG Reference: | AC-2 |

<Specify minimum clearance, access, and citizenship authorized for system.>

|  |  |  |
| --- | --- | --- |
| Minimum Clearance | Minimum Access | Citizenship |
| [ ]  Top Secret[ ]  Secret | [ ]  SAP[ ]  SCI[ ]  Both | [ ]  US[ ]  Other: List citizenship\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

All users are cleared for all information on the system. [ ]  Yes [ ]  No

All users are formally accessed to all information on the system. [ ]  Yes [ ]  No

System Protection Level: PL- Choose

## Account Management Policies

|  |  |
| --- | --- |
| JSIG Reference: | AC-2, AC-3 |

<Insert or reference organizational or system-specific user access policies relevant to information types maintained on the information system. Policies may be placed in an Appendix to the SSP.>

<If group accounts are being used, include your processes or attach a group account procedures document as an Appendix.>

<Sample>

This system is accessed via use of individual accounts and passwords. Accounts are created after personnel complete an Account Request Form, sign a User Acknowledgment Statement and complete General User or Privileged User Training. The ISSM/ISSO and security personnel authorize all system accounts. Passwords are configured via local group policy to be in compliance with the requirements of NIST SP 800-53r4, Control IA-5, with validation and enforcement in accordance with DISA STIG settings. The syntax for a user’s ID is firstname.lastname. Privileged user accounts also contain the role (i.e., “.adm,” “.aud,” “.dta”).

The GSSO, SAP Program Manager, or PSO notifies the ISSM/ISSO to disable or terminate accounts after an individual has been debriefed or a determination is made that account access be withdrawn. Upon notification, the account is disabled for 90 days and then deleted within 12 months unless directed otherwise by the GSSO/PM/PSO.

Group accounts are used on this system. A current list of group members will be maintained. Use of these accounts are tracked using a manual log and accountability checklist that is reviewed during the weekly audits for the system. Shared/group accounts are reviewed quarterly for membership and account requirement.

# GENERAL SYSTEM DESCRIPTION/PURPOSE

|  |  |
| --- | --- |
| JSIG Reference: | PL-2 |

< Provide the mission/purpose of the system. Remember your audience – Keep it brief but understandable. Samples Below>

<Sample 1>

SYSTEM-NAME is a Linux-based periods processing High Performance Computing Environment (HPCE) fielded to process massive amounts of data from compute-intensive applications for a wide variety of use cases such as modeling and simulation and data analysis. The HPCE reduces the computational time for these applications that would take years to process on a single computer down to weeks or days.

The HPCE is designed to be reusable by multiple Department of Defense (DoD) customers with differing datasets or applications. Existing HPC capabilities are limited or unable to process data in a timely manner. Using the HPCE, DoD customers will be able to procure and maintain the computational resources needed for their mission that the HPCE can provide.

<Sample 2>

SYSTEM-NAME is a Windows and Linux-based periods processing system for customers to process project specific data. The analysis clients display mission critical data and safety monitoring information from a variety of real-time sources. Encrypted data sources are received in the room and then decrypted and processed. When accompanied by PSO approval, customer’s systems provide telemetry data directly to their system through KG-135S or equivalent telemetry encryption devices. Sources include range data, telemetry, voice, and video.

<Sample 3>

The organization conducts hardware-in-the-loop (HITL) testing by incorporating actual system hardware into the simulation to develop countermeasures for the protection of aircraft against threat missile systems. HITL provides the capability to test a wide variety of infrared threats which can be mounted on a 5-axis flight motion simulator. A high-fidelity scene projection system provides an infrared image of the aircraft platform to the threat seeker. A countermeasure channel is combined with the aircraft scene projection to enable the testing of flares and laser-based directed infrared countermeasure systems.

## System/Network and Functional Architecture

< Provide a summary description of the system architecture, data flow (to include assured file transfers, e.g., dotted line from network to target system), interconnected systems, operating system(s), virtualized components, and perimeter/information system boundary. The description should describe the data flow in and out of the system, the type of data and what it’s used for, how it is protected. Indicate whether system will operate in periods processing mode and any additional information that describes the system/network. NOTE: If you are periods processing, explain what happens when the drive is not in use. Also address your sanitization procedures in between processing (SEE SAMPLE 4 BELOW).

Describe and provide a diagram of the system architecture (e.g. servers, workstations, printers, etc.) and place it in Appendix B, System/Network Diagram. The diagram must clearly define the authorization boundary. How does this system function? Tell a story! This diagram must also show ALL direct and indirect connections.>

See Network Diagram attached.

<If systems are deployable, list the known/ recurring deployment locations. See Sample 1 below.>

SYSTEM-NAME consists of standalone Windows systems used for aircraft mission planning, which is required to be deployed to other locations in support of weapon system testing outside the base of operation listed on the SSP. The following are known deployments locations:

Nellis AFB Nevada Test Training Range (NTTR)

Edwards AFB, CA

Hollman AFB/White Sands Missile Range (WSMR)

For deployment locations not listed above, an approved PSO transportation/security plan will be uploaded to the BoE on CORE to provide situational awareness to the AO and the location will be added to the SSP at the next annual review if this will be a recurring deployment location. If the security posture of the system will change due to conditions of the system being deployed, an SIA will be required to be submitted to the AO for approval before the deployment of the system.

<Sample 2>

This LAN is a combination of Windows and Linux systems with no outside connection. The Windows systems are used for administrative and development activities. The Linux systems are used for development of the simulation software for hardware-in-the-loop testing. The laptops are used for presentations and connects to an overhead projector in the conference room. One of the systems is a virus scan/air gap, standalone system used to conduct virus scans and verify the media is closed/finalized prior to installation on any computer within this boundary. All transfers are accomplished using the units Assured File Transfer (AFT) procedures.

<Sample 3>

The system consists of a high-end Linux workstation and a Windows workstation used to create wire frame models of aircraft and their Infra-Red (IR) signatures in various flying configurations. Programs running on the systems are used to create a series of simulations that model the IR signatures of each aircraft configuration. The results are compared to known aircraft measurements to validate and verify the modeled signatures. Once validation is complete, run time files are created. These files are transferred to the labs test area using optical media or encrypted hard drives and the units Assured File Transfer (AFT) procedures.

<Sample 4 for Periods Processing>

The SYSTEM-NAME network is a Windows domain composed of Windows servers and Windows clients. The servers contain domain controllers, file servers, and backup servers.

Each program requires a separate set of hard drives utilized for periods processing during mission execution. Each set of program drives are stored separately in GSA-approved safes and protected at the SECRET//SAR level. Prior to being stored in the safe, an audit will be performed on the drives. During the time the drives are not in use, they will be bagged and tagged and audited and patching/antivirus updating will not occur; however, monthly inspections for tamper will be accomplished and logged. On the day of mission execution, mission essential systems are populated with the hard drives. The drives will be updated with any security-relevant patches and antivirus updates. Auditing will be accomplished weekly while the drives are in use.

The system is not connected to any other system or networks. Information transfers will be accomplished via sneakernet for antivirus updates and mission data transfers.

When sanitizing between classifications on IT equipment, the following steps will be followed:

|  |  |
| --- | --- |
| STEP | ACTION |
| 1 | Confirm no classified documentation is left on any peripheral device. If any is found, remove it and handle at the classification level of the processing of the system and report to your ISSM/GSSO. |
| 2 | For laser printers, print 3-5 test sheets of paper to wipe residual toner from the cartridge drum. |
| 3 | Confirm there is no removable media present or inserted. If any is found, remove it and verify it is accounted for or report to the ISSM/GSSO. |
| 4 | Disconnect power source/battery if present and depress power button/switch for 15 seconds. Refer to vendor documentation/LOV/COV for clearing instructions. |
| 5 | Inspect all unsealed ports for presence of suspicious devices (e.g., Dongles, Keyloggers). If anything is found, report to the ISSM and GSSO. |
| 6 | The classified hard drive(s) should be removed after current mission/test is complete and stored. Confirm there is no other fixed storage media present or installed internal to the device. If anything is found, report to the ISSM and GSSO. |
| 7 | Inspect equipment for obvious signs of tampering, modification, and presence of unauthorized components. If anything is found, report to the ISSM and GSSO. |

NOTE: Steps 1&2 are for peripheral devices and 3-7 are for all equipment including the peripheral devices.

All sanitization between periods processing will be documented to show the procedures that have been followed, the date, and the name of the individual sanitizing the system(s).

ALL Secret Collateral and Secret//SAR equipment and media used in the SAPF in a periods processing environment must be retained in a SAP environment. All Secret Collateral and Secret//SAR equipment and media will be destroyed using approved procedures for the destruction of SAP equipment and media.

All media transfers will be accomplished using the units Assured File Transfer (AFT) procedures.

<If Special Test Equipment is used, add the following:>

Some of the equipment used for periods processing will be Special Test Equipment (STE). Some of the equipment has been built in-house and the SME is responsible for the sanitization procedures. The Letter of Volatility (LOV) or Certificate of Volatility (COV) provided by the vendor or manufacturer of the equipment is the source documentation which provides the approved method of clearing/sanitization each specific type of equipment. If an LOV/COV is unavailable for a particular device, the appropriate SME will develop and formalize clearing/sanitization procedures. The unit ISSM provides final approval of the procedures prior to implementation. All vendors’ LOVs/COVs or other documented sanitization procedures will be available to sanitization personnel whether hard or soft copy.

<NOTE: Consider adding that the system/monitor labels will be replaced with the appropriate level of operation.>

Compliance with this sanitization plan ensures that the equipment is properly controlled, sanitized, verified, and documented prior to periods processing at different levels. The following steps outline sanitization procedures for test equipment.

|  |  |
| --- | --- |
| STEP | ACTION |
| 1 | Perform LOV/COV procedures as directed by the vendor/manufacturer. |
| 2 | Inspect outer shell, case, or housing for any indication of tampering. |
| 3 | Confirm there is no removable media present or inserted. If any is found, remove it and verify it is accounted for or report to the ISSM/GSSO. |
| 4 | Inspect all unsealed ports for presence of devices. Report any findings to your ISSM/ISSO. |
| 5 | Document the sanitization of Special Test Equipment in the unit log. |

The above sanitization instructions are for STE being used in periods processing that stay within secure channels. For any STEs going out of secure channels, approved SAPCO procedures must be followed.

## User Roles and Access Privileges

< Identify the types of system users (e.g. Privileged User, General User, Database Administrator, Data Transfer Agent) and describe their access/privileges.>

<Sample>

|  |  |
| --- | --- |
| User Role | Access Privileges |
| Administrators (.adm) | Performs system administration duties |
| Auditors (.aud) | Runs audits and has access to the Security event logs |
| Engineers/Analysts | Performs the duties of testing |
| Data Transfer Agents (.dta) | Transfers data between systems |
| General Users | No elevated privileges/rights to network resources |

Privileged accounts have the ability to make system and security changes.

**Administrative** accounts are restricted to System Administrators (SA) who perform system maintenance and create and administer user accounts. Administrators must have a working knowledge of system functions, security policies, technical security safeguards and operational security measures. All administrators are assigned to the administrators group and the user name will include the suffix of “.adm.” SAs must have separate and unique accounts with administrative privileges for performing any administrative functions. The use of administrator accounts will be audited. This account will only be used when necessary.

**Auditor** accounts are used as separate accounts and will include the suffix of “.aud.” Auditor accounts will be used for event log auditing of systems and use of the accounts will be audited.

**Data Transfer Agent (DTA)** accounts are privileged roles and assigned to select personnel who have been identified in writing. All activities performed by these account holders will be documented in the maintenance log and on the Data Transfer Log.

**General Users** are the basic user accounts created in account management. They are non-privileged users and do not have the ability to perform any actions that require elevated privileges.

## User-Developed Software

|  |  |
| --- | --- |
| JSIG Reference: | CM-7(5), CM-10(1), CM-11, CM11(2), SA-10(1), SA-11, SA-15, SI-7(14) |

<Not a requirement for this section but, if it fits your system, recommend its use. Sample below.>

General users are allowed to compile and develop software on the system. All compile actions will be monitored and audited per AC-6(9) in the system SCTM. Users may move their compiled executables and libraries to local directories or network shares where DAC policy permits execution.

Users are prohibited from introducing machine-executable code or source code from sources without approval from ISSM/ISSO. Users will be required to declare what software they intend to develop and compile on the IS for the intended test period. The users must also state if their software will access any network resources, to include ports, protocols, and services. Any deviations from a user’s original stated intent during the period will need to be approved and documented by the ISSM/ISSO.

If users generate an installer package, an administrator will be required to install it.

# INTERCONNECTIONS/INFORMATION SHARING

|  |  |
| --- | --- |
| JSIG Reference: | AC-4, AC-17, AC-21, CA-3, PL-2 |

## Direct Network Connections

<List all Direct Network Connections. An ATC or ISA is required for all direct connections. Before adding a direct connection, ensure each direct connected system can process all PIDs listed on each ATO. See Sample Direct Connection below.>

|  |
| --- |
| [ ]  This system does **not** connect to any other system.  |
| [ ]  This system connects with the following network(s) or system(s).\*\* |
| **SYSTEM NAME** | **ORGANIZATION** | **CLASSIFICATION & COMPARTMENTS** | **ACCREDITED BY** |
| EXODUS | NAWCWD | SECRET//SAR | NAVY |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*\*\*NOTE: Direct network connections with external organizations, whether internal or external to the facility must be addressed in an MOU and/or ISA.*

## Indirect Connections

*<*This section refers to information received through means other than a direct connection, e.g. “Sneaker Net.” Most will use NIPR for AV updates. See Sample Indirect Connections below.*>*

|  |
| --- |
| [ ]  This system does not accept or process data stored on any other systems. i.e. No input from other systems are allowed onto this system. |
| [x]  This system accepts and processes data stored on media created on the following system(s) as part of its core mission processes: Complete information below. |
| **SYSTEM NAME** | **CLASSIFICATION & COMPARTMENTS** | **ACCREDITED BY** | **TRANSFER METHOD**  |
| NIPRNet | Unclassified | DoD | CD/DVD, External HD using approved one-way transfer method (Tableau) |
| SystemName L-XXXXX | SECRET//SAR | AFLCMC | CD/DVD |
|  |  |  |  |

<Complete for all systems that you will copy data to (i.e., CV2) and the method (i.e., CD/DVD or External Hard Drives).  Accredited by will usually be DoD, OSI PJ, SAF/AAZ, AFTC AO, or other MAJCOM/Center AOs.  See Sample Out-going Indirect Connections below.>

|  |
| --- |
| [ ]  Data from this system is NOT shared or distributed to any other systems. i.e., No output from this system goes into another system. |
| [x]  Data stored on media created on or used on this information system is distributed for use on the following system(s): |
| **SYSTEM NAME** | **CLASSIFICATION & COMPARTMENTS** | **ACCREDITED BY** | **TRANSFER METHOD**  |
| CV2 | SECRET//SAR | SAF/AAZ | CD/DVD, External Self-Encrypted Drives |
| SystemName L-XXXXX | SECRET//SAR | AFLCMC | CD/DVD |
|  |  |  |  |
|  |  |  |  |

## Memorandums and Agreements

|  |  |
| --- | --- |
| JSIG Reference: | AC-20, CA-3 |

<Include Memorandums of Understanding (MOU), Memorandums of Agreement (MOA), Co-Utilization Agreements (CUA), Authorizations to Connect (ATC) and Interconnection Security Agreements (ISA)>

[ ]  This information system does not require any MOU/MOA, CUA, ATC, or ISA for interconnection or operation.

[ ]  This information system requires an MOU/MOA, CUA, ATC, and/or ISA for interconnection or operation.

*<*Copies of the MOU/MOA, ATC, and/or ISA referenced in this table must be available to the SCA for review during the verification and validation testing. NOTE: In the event of more than one MOU/MOA/CUA/ATC/ISA, copy table and complete individually for each document.>

|  |  |
| --- | --- |
| **Subject of Agreement** |  |
| **Date of Agreement** |  |
| **POC Name** |  |
| **Organization** |  |
| **Contact (phone or e-mail)** |  |

1. Acronyms

AFT Assured File Transfer

ATO Authorization to Operate

CI Controlled Interface

CNSSI Committee on National Security Systems Instruction

CDS Cross Domain Solution

CSA Cognizant Security Authority

CUA Co-Utilization Agreement

ID Identification

ISA Interconnection Security Agreement

ISSM Information System Security Manager

ISSO Information System Security Officer

IT Information Technology

LAN Local Area Network

MOU Memorandum of Understanding

NIST National Institute of Standards and Technology

OMB Office of Management and Budget

PIT Platform IT

POA&M Plan of Action and Milestones

POC Point of Contact

SP Special Publication

SCA Security Control Assessor

SCTM Security Controls Traceability Matrix

SSP System Security Plan

WAN Wide Area Network

1. System/network diagram

See attached System/Network Diagram <or place it here but for our package submissions, the diagram will be a separate part of the package submission. If attached, refer to the Diagram but recommend the exact filename is not listed as it’s another BoE document that would have to be changed when the attached is updated. Ensure the diagram is classified appropriately.>

<You will need a topology diagram to show boundary and all connections (direct and indirect) as well as data flow and data type. The diagram should match your hardware list. You can show one workstation and place a “x5” for 5 workstations. Make sure your arrow directions for indirect connections are accurate so you don’t show a H2L transfer that’s not being done on your system. >

<Sample Standalone Workstation>



<Sample Isolated Network>



<Sample Network with Direct Connection>



1. Assured File Transfer Procedures

See attached Assured File Transfer (AFT) Procedures. <or place it here. If attached, refer to the AFT Procedures but recommend the exact filename not be listed as it’s another BoE document that would have to be changed when the attached is updated.>

<Include Assured File Transfer (AFT) procedures (e.g. high to low; low to high) or reference the SOP here. You can remove this Appendix and refer to your AFT procedures in the SCTM (AC-4) and add it to your SCTM Supporting Documentation..>

1. SECURITY CONTROL TRACEABILITY MATRIX

See attached SCTM. <Refer to the SCTM but recommend the exact filename not be listed as it’s another BoE document that would have to be changed when the attached is updated.

1. HARDWARE LIST

See attached Hardware List <or place it here but for our package submissions, the HW List will be a separate part of the package submission. If attached, refer to the HW List but recommend the exact filename not be listed as it’s another BoE document that would have to be changed when the attached is updated.>

<HW List MUST match system diagram (Appendix B) for all systems and quantities!>

<If no EOL/EOS is found, place “No EOL” in block. If there is an EOL date, put date in block. Any EOL/EOS hardware should be on your POA&M for SA-22. If the warranty for hardware is expired, it is not considered EOL if there is extended support or paid support. Only EOL or EOS if no more support is provided.>

| **Device Type** | **Manufacturer** | **Model** | **Serial Number** | **EOL/EOS** | **Function/Purpose** |
| --- | --- | --- | --- | --- | --- |
| Workstation | Dell | Optiplex 755 | 1HS36H1 | 31 Dec 21 | Creation of reports and analyzing test data. |
| Server | Dell | PowerEdge R640 | 6DLL525 | No EOL | File Server |
| Printer | HP | 8500 | KLH2315 | No EOL | Printing Documents |

1. SOFTWARE LIST

See attached Software List <or place it here but for our package submissions, the SW List will be a separate part of the package submission. If attached, refer to the SW List but recommend the exact filename not be listed as it’s another BoE document that would have to be changed when the attached is updated.

The EOL/EOS will have to be included. Any EOL/EOS software should be on your POA&M for SA-22. If there is extended support or paid support, it is not considered end-of-life. Only EOL or EOS if no more support is provided.

Also include which systems the software is installed on if your boundary includes more than one system. If the software listed is installed on all systems, state that in the System block so the assessor will know what STIG-compliance and vulnerability scans they should expect to see submitted. Patches, drivers and software installed by the OS (e.g. Microsoft Visual C+++ 20XX Redistribution) aren’t required to be listed on the SW List. Any software with a STIG associated with it needs to be listed. Your SW List should match your STIG applicability list (required BoE).>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Publisher** | **Application Name** | **Version** | **EOL/EOS** | **System** | **Purpose** |
| Microsoft | Windows 10 | 1909 | 10 May 22 | All workstations | Operating system |
| Microsoft | Server | 2019 Standard | 9 Jan 29 | AppSvr01 | ACAS Server for system vulnerability scans. |
| Adobe | Acrobat Standard DC 2015 | 11.0 | 7 Jul 20 | All workstations | Office automation |

1. User AgreementS

See attached General and Privileged User Agreements. <or place it here. If attached, refer to the User Agreements but recommend the exact filenames not be listed as it’s another BoE document that would have to be changed when the attached is updated.>

<Provide general and privileged user access agreements and acknowledgement of responsibilities. Ensure the agreements provided reflect the current versions in use and that they include a formal sanctions process for non-compliance in accordance with JSIG (PS-8). >

1. NETWORK PORTS LISTING

See attached Network Ports Listing. <or place it here but for our package submissions, the Network PPS Listing will be a separate part of the package submission. If attached, refer to the Network PPS Listing but recommend the exact filename not be listed as it’s another BoE document that would have to be changed when the attached is updated.>

<For Direction, show “inbound,” “outbound,” or “bi-directional”>

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Service** | **FROM** | **TO** | **Port** | **Protocol** | **Direction** | **Notes** |
| **Hostname or IP** | **Hostname or IP** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |