

Appendix C

AISSP Outline

This outline provides the basis for preparing an AIS Security Plan (**AISSP**). The annotated outline, with prompts and instructions, will assist **ISSRs** in preparing a plan that includes necessary overviews, descriptions, listings, and procedures. It will also assist in covering the requirements contained in this **NISPOM** Supplement. In preparing the **AISSP**, any information that does not appropriately fit under a subtitle may be placed under a main title. For example, a hardware list or references to a hardware list will be placed under the 4.0 AIS HARDWARE heading. For changes to an existing plan that do not require revision of the entire plan, provide name and date of the plan to be modified, date of changes on each page, and cross reference to the plan's applicable paragraph numbers. (For changes, only the change pages with the applicable plan name and date need to be sent to the **CSA**.)

Table Of Contents

1.0	INTRODUCTION		
	1.1 Administration		
	1.2 Purpose and Scope		
2.0	SAPF DESCRIPTION		
	2.1 Physical Environment		
	2.2 Floor Layout		
	2.3 SAPF Access		
3.0	AIS DESCRIPTION		
	3.1 General Information		
	3.2 Configuration and Connectivity		
	3.3 User Access and Operation		
	3.4 Audit Trail		
4.0	AIS HARDWARE		
	4.1 Labeling Hardware		
	4.2 Maintenance Procedures		
			4.3 Hardware Sanitization and Destruction
			4.4 Hard ware Transport and Release
			4.5 Hardware Control and Audit Trails
		5.0	AIS SOFTWARE
			5.1 Authorized Software
			5.2 Software Procedures
		6.0	DATA STORAGE MEDIA
			6.1 Labeling and Storing Media
			6.2 Media Sanitization and Destruction
			6.3 Media Transport and Release
			6.4 Media Control
		7.0	AIS SECURITY AWARENESS
		8.0	GLOSSARY OF TERMS

1.0 INTRODUCTION

This section will describe the purpose and scope of the **AISSP**. It may include any topic intended to help the reader understand and appreciate the purpose of the AISSP. Pertinent background information may also be presented to provide clarity.

1.1 Security Administration.

Provide the name and date of this plan and indicate whether it is an original or revised plan.

Specify the cognizant Customer Program Office whose activity the AIS will support and the contract number(s), if applicable.

Specify the Provider's name and address. Identify the location of the AIS equipment (including the building and room numbers(s)).

Provide the names of the Provider's program manager, **ISSR**, alternate(s). Also provide their secure and **unsecure** telephone numbers and their normal office hours.

Provide an organizational structure showing the name and title of **all** security management levels above the ISSR.

Provide joint-use information if applicable.

1.2 Purpose and Scope.

The plan will describe how the Provider will manage the security of the system. Describe the purpose and scope of this AIS.

2.0 SAPF DESCRIPTION.

This section will provide a physical overview of the AIS SAPF (including its surroundings) that is used to secure the Customer's program activities. It **will** include information about the secure environment required to protect the AIS equipment, software, media, and output.

2.1 Physical Environment.

State whether the SAPF is accredited or approved to process and store classified information, who accredited or approved it, the security level, and when approved. State whether the SAPF is approved for open or closed storage.

Specify whether the storage approval is for hard disk drives, diskettes, tapes, printouts, or other items.

State whether the approval includes unattended processing.

2.2 Floor Layout.

Provide a floor plan showing the location of AIS equipment and any protected wire lines. (This may be included in a referenced appendix.) The building and room number(s) will match the information provided in the hardware listing (see 4.0).

2.3 **SAPF** Access.

Describe procedures for controlling access to the AIS(S) to include: after hours access, personnel access controls, and procedures for providing access to uncleared visitors (e.g., admitting, sanitizing area, escorting).

2.4 TEMPEST.

If applicable, describe TEMPEST countermeasures.

3.0 **AIS DESCRIPTION**

This section will provide a detailed description of the system and describe its security features and assurances.

Describe variances and exceptions.

3.1 **General Information**

Provide a system overview and description.

Specify clearance level, formal access (if appropriate), and need-to-know requirements that are being supported.

Identify the data to be processed including classification levels, compartments, and special handling restrictions that are relevant.

State the mode of operations.

Indicate the AIS's usage (in percent) that will be dedicated to the Customer's activity (e.g, periods processing).

3.2 **Configuration and Connectivity.**

Specify whether the AIS is to operate as a stand-alone system, as a terminal connected to a mainframe, or as a network.

Describe how the AIS or network is configured. If a network, specify whether it is a unified network or interconnected network. Describe the security support structure and identify any specialized security components and their role.

Identify and describe procedures for any connectivity to the AIS(S). Indicate whether the connections are to be classified or unclassified systems.

Provide a simplified block diagram that shows the logical connectivity of the major components (this may be shown on the floor layout if necessary-see 2.2). For AISS operating in the compartmented or multilevel modes an information flow diagram will be provided.

If applicable, discuss the separations of classified and unclassified AISS within the SAPF.

Indicate whether the AIS is configured with removable or nonremovable hard disk drives.

Describe the configuration management program. Describe the procedures to ensure changes to the AIS require prior coordination with the ISSR.

3.3 User Access and Operation.

Describe the AIS operation start-up and shut-down (mode termination). Provide any unique equipment clearing procedures.

Discuss all AIS user access control (e.g., log-on ID, passwords, **file** protection, etc.).

Identify the number of system users and the criteria used to determine privileged access.

If the mode is other than dedicated, discuss those mechanisms that implement DAC and MAC controls.

Discuss procedures for the assignment and distribution of passwords, their frequency of change, and the granting of access to information and/or files.

Indicate whether AIS operation is required 24 hours per day.

Discuss procedures for after hours processing. State whether the AIS(S) are approved for unattended processing.

Discuss procedures for marking and controlling AIS printouts.

Discuss remote access and operations requiring specific approval by the CSA.

Discuss procedures for incident reporting.

3.4 Audit Trails.

If applicable, discuss the audit trails used to monitor user access and operation of the AIS and the information that is recorded in the audit (rail. State whether user access audit trails are manual or automatic.

Identify the individual who will review audit trails and how often.

Describe procedures for handling discrepancies found during audit trails reviews.

4.0 AIS HARDWARE

This section will describe the AIS hardware that supports the Customer's program. This section will provide a listing of the AIS hardware and procedures for its secure control, operation, and maintenance.

Provide a complete listing of the major hardware used to support the Customer's program activities. This list may be in tabular form located either in this section or a referenced appendix. The following information is required for all major AIS hardware: nomenclature, model, location (i.e., building/room number), and manufacturer.

Provide a description of any custom-built AIS hardware,

Indicate whether the AIS hardware has volatile or nonvolatile memory components. Specifically, identify components that are nonvolatile.

If authorized, describe procedures for using portable devices for unclassified processing.

Identify the custodian(s) for **AISs**.

4.1 Labeling Hardware.

Describe how the AIS hardware will be labeled to identify its classification level (e.g., classified and unclassified AISS collocated in the same secure area).

4.2 Maintenance Procedures.

Describe the maintenance and sanitization procedures to be **used** for maintenance or repair of defective AIS hardware by inappropriately cleared personnel.

4.3 Hardware Sanitization and Destruction.

Describe the procedures or methods used to sanitize and or destroy AIS hardware (volatile or nonvolatile components).

4.4 Hardware Movement.

Describe the procedures or receipting methods used to release and transport the AIS hardware from the SAPF.

Describe the procedures or receipting methods for temporarily or permanently relocating the AIS hardware within the SAPF.

Describe the procedures for introducing hardware into the SAPF.

4.5 Hardware Control and Audit Trails.

Describe all AIS hardware maintenance logs, the information recorded on them, who is responsible for reviewing them, and how often.

5.0 AIS SOFTWARE

This section will provide a listing of all the software that supports the Customer's program. It will also provide procedures for protecting and using this software.

5.1 Authorized Software.

Provide a complete listing of all software used to support the Customer's program activities. This list may be in tabular form and may be located either in the section or in a referenced appendix. The listing will also include security software (e. g., audits software, anti-virus software), special-purpose software (e.g., in-house, custom, commercial utilities), and operating system software. The following information is required for AIS software: software name, version, manufacturer, and intended use or function.

5.2 **Software Procedures.**

Indicate whether a separate unclassified version of the operating system software will be used for maintenance.

Describe the procedures for procuring and introducing new AIS software to support program activities.

Describe the procedures for evaluating AIS software for security impacts.

Describe procedures for protecting software from computer viruses and malicious code and for reporting incidents.

6.0 **DATA STORAGE MEDIA**

This section provides a description of the types of data storage media to be used in the Customer's program and their control.

6.1 **Labeling and Storing Media.**

Describe how the data storage media will be labeled (identify the classification level and contents).

Discuss how classified and unclassified data storage media is handled and secured in the SAPF (e.g., safes, vaults, locked desk).

6.2 **Media Clearing, Sanitization, and Destruction.**

Describe the procedures or methods used to clear, sanitize, and destroy *the data storage* media.

6.3 **Media Movement.**

Describe the procedures (or receipting methods) for moving data storage media into and out of the SAPF.

Describe the procedures for copying, reviewing, and releasing information on data storage media.

6.4 **Media Control.**

Describe the method of controlling data storage media.

7.0 **AIS SECURITY AWARENESS PROGRAM**

Discuss the Provider's security awareness program.

Indicate that the AIS users are required to sign a statement acknowledging that they have been briefed on the AIS security requirements and their responsibilities.

8.0 **GLOSSARY OF TERMS**