S/390 LOGICAL PARTITION

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 2

4 March 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

This page is intentionally left blank.

SUMMARY OF CHANGES

Changes in this document since the previous release (Version 2, Release 1, dated July 2003) are listed below.

GENERAL

Updated cover page, headers, and footers with the newest version of the Section 1 template.

SECTION 1

Made changes based on STIG consistency efforts.

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

The *S/390 Logical Partition Security Technical Implementation Guide* defines the technical criteria necessary to implement Mission Assurance Category (MAC) II Sensitive functionality within DISA non-classified multiple partitions and classified partitions. This document does not define policy, but documents the procedures and parameters necessary to implement policy. Policy serves no value if it cannot be technically implemented.

Many of the sites running S/390 are doing so on processors capable of executing multiple environments concurrently. In addition to the security required within S/390, additional requirements are necessary to ensure the integrity of each environment. Also, controls will be in place to ensure the separation of data with different classification levels.

Each manufacturer uses a different term for describing a Logical Partition. Amdahl uses the term domain. Hitachi Data Systems (HDS) and IBM both use the term LPAR. Throughout this document, LPAR is used generically to refer to any manufacturer's logical partition.

When implementing security within the S/390 operating platform, or within any platform, essentially three criteria must be considered — confidentiality, integrity, and availability. For the purposes of this document, each is defined as follows:

- **Confidentiality:**

  Assurance that information is not disclosed to unauthorized entities or processes. Confidentiality encompasses *least privilege*. *Least privilege* says that users have only the authority to access those resources necessary to perform their functions.

- **Integrity:**

  Defined as the assurance that resources, to include data, are the same as that in the source and have not been exposed to accidental or malicious alterations or destruction.

- **Availability:**

  Characterized as the assurance that resources (including data) are in the place, at the time, and in the form needed by the user.

This document defines the requirements, standards, controls, and options that must be in place for each LPAR in a processing complex to comply with the MAC II Sensitive requirements. The site may implement additional security as necessary to allow multiple partitions to exist on the same physical box without risk to the integrity of the LPAR.

It should be noted that FSO support for the STIGs, Checklists, and Tools is only available to DOD Customers.

1.2 Scope

The requirements set forth in this document are for S/390 LPARs and for the hardware and software used to support LPARs at the DOD sites.

1.3 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II Sensitive level, containing sensitive information.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**," indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1.1. Vulnerability Severity Code Definitions

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site, http://www.cert.mil.

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank.

2. LOGICAL PARTITIONING GENERAL CONSIDERATIONS

2.1 What Is Partitioning

2.1.1 Physical Partitioning

Physical partitioning is a method of dividing up the resources of a hardware environment by assigning the components to one or more physical processors. These assignments are done at the hardware level. Reconfiguration of resources can be done dynamically.

The specifics of physical partitioning have certain requirements. Sufficient hardware resources will exist to permit more than one physical machine.

For example, the processor will possess more than one CPU, and it will be defined with the processor and divided so that each side has its own physical definition. It would require at least two strings of DASD, each with its own controller (one for each processor). Each channel would have to be assigned only one of the CPUs. It is possible to cross-cable the DASD controllers, thereby enabling joint access from each processor. This is not being addressed in this document as this portion on physical partitioning is meant as an example.

The end result of using physical partitioning is that the design is static. Making even minor changes may require a shutdown of a partition. The advantage is that each partition is discrete. It is impossible for one system to have any effect on another unless there is cross cabling. From the user's aspect, these appear to be two different physical machines.

2.1.2 Logical Partitioning

Logical partitioning is a method of executing multiple instances of an operating system concurrently on the same processor complex without the requirement of an extra layer of software (e.g., VM). This is now possible in many cases by advances in both hardware and software. In many instances it is also possible to physically partition the hardware of a computer. However that capability will not be addressed in this document.

The ability to run multiple LPARs is available on many models of IBM and IBM-compatible mainframes. This feature has different names on different processors:

Multiple Domain Feature (MDF) – Amdahl
Multiple Logical Processor Facility (MLPF) – Hitachi Data Systems (HDS)
Processor Resource/Systems Manager (PR/SM) – IBM

Each product essentially performs the same functions, allowing simultaneous execution of multiple operating system images (e.g., OS/390, VSE, and UTS).

This is done by dividing the physical processor complex into logical processing environments that consist of main storage, channels, operator facilities, and logical and/or physical processors used to permit the operation of a System Control Process (SCP).

2.2 How Partitioning Works

For the purpose of this document, **hardware** refers to the physical processor and the physical attachments and devices that control them. Defining the actual hardware resources and their controllers performs the partitioning of the hardware. The hardware is defined using the TSO/E ISPF dialog Hardware Configuration Definition (HCD) from which the output is stored on a drive internal to the processor complex. For a VM LPAR, the IOCP utility is used to create the IOCDS, which defines the hardware configuration.

When **software** partitioning is referenced, this relates to the programs that define the logical devices to the operating system and enable the software to access the hardware.

2.2.1 Hardware Functions

The processor complex is designed so the resources within a machine (e.g., CPUs, channels, and memory, etc.) may be assigned to a specific LPAR. For example, a machine consisting of three CPUs may be divided into two or more logical partitions (LPARs). The actual number of LPARs depends upon the model and manufacturer of the processor complex.

2.2.1.1 Input/Output Configuration Data Set (IOCDS)

The CPU requires a way of identifying the hardware attached to it. Without a way to identify the hardware, the processor has no way to identify its resources.

Creating an Input/Output Configuration Data Set (IOCDS) does this. When this data set is created, each of the available resources is divided among the number of partitions being defined.

This information is created by processing the contents of the Input/Output Definition File (IODF) that contains the identifying statements for each of the resources. These include everything from channel definitions to device descriptions and unit addresses.

The IOCDS is written to the processor's internal hard drive. This is then loaded during a Power On Reset (POR) into the Hardware Save Area (HSA). The HSA is the location in storage containing the information the system uses to identify its resources.

The IOCDS is used in all of the IBM-compatible 370/390 processors, although some minor differences exist from platform to platform.

In the case of IBM and Hitachi Data Systems, only one IOCDS exists for each physical machine, and it contains all the available resources for all the partitions.

When using Amdahl hardware, one major difference exists. Amdahl uses a separate IOCDS for each logical partition.

All maintenance that will be made to the IOCDS is done by applying changes to the IODF, generating a new IOCDS using HCD, and loading the new IOCDS to the Hardware Save Area

(HSA) using IOCP. *Section 2.2.1.3, Hardware Configuration Definition (HCD) Program,* discusses HCD.

- *Unauthorized reading and writing of IOCDS files will not be allowed.*

2.2.1.2 Input/Output Configuration Program (IOCP)

The purpose of the IOCP is to process the Input Output Definition File (IODF) containing the hardware definitions. The input is converted to machine-readable format, and the definition is saved in the IOCDS.

The input file is made up of the macros and parameters necessary to define the hardware channel subsystem. The hardware channel subsystem is the physical layout of all the devices on the system and their addresses.

When HCD invokes the IOCP program, the program runs syntax checks against the IODF data set. If the file is processed with no errors, the output data set IOCDS is then created and loaded to the Hardware Support Processor. In order to load the IOCDS into the Hardware Save Area, an **ACTIVATE** is performed.

The integrity of the IOCDS is critical to the system. If this file becomes corrupted or is changed without anyone’s knowledge, the results could be catastrophic. Because of this, the ability to execute the IOCP will be restricted to only the Systems staff.

- *The IAO will create and maintain ACP data set rules for the* ***IOCP*** *program. The rules will restrict access to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*

2.2.1.3 Hardware Configuration Definition (HCD) Program

Beginning with MVS/ESA 4.3, IBM implemented a TSO/E ISPF dialog known as Hardware Configuration Definition (HCD), which is used to create and maintain hardware configurations for Central Processor Complexes. HCD is able to make changes simultaneously to both the channel subsystem and the operating system, thus eliminating the redundancy of creating and maintaining two source library members. In addition, HCD performs the verification of the hardware and software definitions as they are processed prior to writing the output. When combined with the Dynamic I/O Reconfiguration Management function, the changes can be implemented immediately, without requiring a POR or an IPL. For VM LPARs, the IOCP utility is used to perform the same function as HCD.

- *The IAO will ensure that the IOCP utility (ies) is (are) defined using the* ***PROGRAM*** *resource class and restricted to authorized personnel. The IAO will also ensure that access to the program is logged.*

HCD keeps track of hardware configurations using a VSAM file known as the Input/Output Definition File (IODF). A single IODF can contain definitions for several processors or LPARs and several MVS systems. HCD uses two versions of IODF to apply changes in order to ensure minimal downtime. The two versions of the IODF are as follows:

- The first version is referred to as the **work** IODF. The naming convention for the work IODF should be **SYS3.IODFxx.WORK** (where **xx** is site dependent). HCD enables authorized personnel to view and maintain hardware configurations in the work IODF. The work IODF will be ACP protected. All access and update authority will be restricted to only systems personnel and authorized users. HCD uses the work IODF to generate the second IODF. The work IODF is not suitable for selection during IPL or dynamic activation. As a result, a second version of the IODF is created and referred to as the production IODF.

    - The production IODF is a *read only* file that contains the current hardware configuration, and is used by HCD to generate and load the IOCDS. It is recommended that the naming convention for the production IODF be **SYS3.IODFxx**, where **xx** is site dependent. This IODF will be ACP protected and should be located on the same DASD device as **SYSn.IPLPARM**. All access and update authority will be limited to only systems personnel and authorized users. It is recommended that one IODF be created for the entire environment. The production IODF will be placed on the production IODF device that is pointed to by the load parm (L2) on the OPRCTL/SYSCTL frame on the hardware system/management console, depending on the machine at IPL time. The production IODF will be accessible by all systems whose configuration is supported by that IODF. If all systems cannot access the IODF volume, a copy can be placed on a device available to the other systems. SMS should not be used to manage the production IODF.

In order to create a production IODF, the build IODF option on the Activate Configuration Data panel is selected. Once the production IODF is created, the build IOCDS option on the same panel is used. Finally, the IOCDS can be loaded and activated using the same panel. As mentioned in a prior section, IOCP is used by HCD to perform these functions. For security purposes, a data set profile will be set for all data sets used by HCD.

- *The IAO will create and maintain ACP data set rules for the **IODFxx.WORK** data set. The rules will restrict access to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*
- *The IAO will create and maintain ACP data set rules for the **IODFxx** data set. The rules will restrict access to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*

Two profiles will also be defined in the **FACILITY** class to allow management of the IOCDSs and IPL attributes for a S/390 microprocessor cluster:

- **CBD.CPC.IPLPARM**

  Queries and updates the **IPLADDR** and **IPLPARM** values for IPL.

  - **CBD.CPC.IOCDS**

  Queries and updates IOCDS control information.

- *The IAO will create and maintain ACP rules that restrict read and update access of* ***CBD*** *prefixed resources to authorized personnel. The logging option will be turned on for all access.*

As part of the creation of the production IODF and the IOCDS, a processor token is generated which is loaded into the HSA. This processor token is used by the system at IPL time to synchronize the configuration in the HSA with the production IODF to determine whether hardware and software changes are allowed. If the tokens match, the system will IPL and changes will be allowed. If not, the system will still IPL but will not allow changes.

An equivalent **SYS3.IODFxx.ACTLOG** will be created and used for each IODF file. This file is used to keep track of changes made to the corresponding IODF. In order to identify to MVS the IODF that is in use, an entry is placed in the **SYS1.PARMLIB** member **LOADxx** that defines the currently active IODF. (IBM recommends that the **LOADxx** member be placed in the library **SYSn.IPLPARM** because **SYSn.IPLPARM** is always checked before **SYS1.PARMLIB**.) In either case, the **SYS1.PARMLIB** and **SYSn.IPLPARM** libraries will be ACP-protected. All access and update authority will be limited to only systems personnel.

Dynamic I/O Reconfiguration is the ability to select a new I/O configuration definition without having to perform a POR of the hardware or an IPL of the system. It enables installation personnel to add, delete, or modify the definitions of channel paths, control units, and I/O devices to the software and hardware configurations. The I/O configuration definitions can be changed for both the hardware and software or for the software only. In order for a device to be available for Dynamic I/O Reconfiguration, the device must be defined through HCD as a dynamic device in the IODF, and must be represented to the software by a unit information module (UIM). The UIM is used to determine if a device supports Dynamic I/O Reconfiguration.

As mentioned earlier, a UIM contains the information and rules that HCD uses to validate and process I/O device definitions. It should also be noted that at IPL time or during dynamic configuration changes, the system invokes a UIM to build the Unit Control Blocks (UCBs).

An alternative method of invoking dynamic reconfiguration is by using the MVS **ACTIVATE** command from an MCS console. When an **ACTIVATE** command is issued, the I/O supervisor calls *jobname* **IEASYSAS**, *stepname* **IOSAS**, to assist in the activate procedure. **IOSAS** requires *read* access to the IODF files. Since the default entry for **IOSAS** in the PPT is **PASS**, ACP checking should occur. To ensure that the activate procedure can complete successfully, do one of the following:

- Place the **IOSAS** task into the ACP Started Task table and indicate that the user is privileged.

- Define the IODF data sets to the ACP with *read* access.

- Add **IOSAS** as an entry in the Started Procedures table with a valid userid. This userid will be granted *read* access to **SYS1.NUCLEUS** and the IODF data sets.

In order to allow use of the sysplex-wide activate function, the following two profiles will be defined in the **OPERCMDS** class:

- **MVS.DISPLAY.IOS**

  Read authority to authorized personnel to display the IOS configuration requests.

  - **MVS.ACTIVATE**

  Update authority to activate configuration changes to only systems personnel and authorized users.

HCD provides the capability to obtain reports about the configuration in use. Reports that may be obtained include printouts of activity logs and a comparison of IODFs, as well as a printed configuration of the Channel Subsystem and OS system view. To obtain these reports, use either the Print or Compare Configuration Data Panel or the Print Configuration Reports. It is recommended that these reports be restricted to authorized personnel.

- *The Site will maintain an **ACTLOG** log data set for each IODF.*
- *The IAO will create and maintain ACP rules restricting access to the **ACTLOG** log data sets to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*
- *The IAO will create and maintain ACP rules restricting access to authorized personnel for the following data sets:*

SYS1.SCBDHENU	**(FMID)**
SYS1.SCBDCLST	**(CLIST)**
SYS1.SCBDPENU	**(PANELS)**
SYS1.SCBDMENU	**(MESSAGES)**
SYS1.SCBDTENU	**(TABLES)**

- *The logging option will be turned on for all UPDATE and/or ALTER access to the above files.*
- *The Site will place the production and backup IODF files on the same disk pack.*
- *The IAO will create and maintain ACP rules restricting access to the* ***ACTIVATE*** *command to authorized personnel. The logging option will be turned on for all accesses.*

2.2.1.4 Processor Resource/Systems Manager

Processor Resource/Systems Manager (PR/SM) is a feature of IBM mainframes. PR/SM enables a Central Processor Complex (CPC) to be divided into one or more logical partitions (LPs). The model number of the machine determines the maximum number of LPARs that a machine may be divided into.

LPs operate independently. Each can be defined to the CPC as either dedicated or shared, but not both. When an LP is activated in a dedicated mode, it is assigned a physical CP (Central Processor). As a result, that CP handles all processing requirements for that LP. LPs can also be defined as shared. When an LP is activated in a shared mode, PR/SM allows the LP to share CPUs from the shared pool, depending on the model number. CPs that are shared are placed into a pool. When an LP is activated in a shared mode, PR/SM allows the LP to share CPUs from the shared pool. The PR/SM scheduler is responsible for dispatching it to the LP. The number of shared CPs for a complex is equal to the total physical number on the system, less the number of CPs assigned to dedicated partitions.

Prior to LP activation, central storage and external storage are defined for the LP. This is done through the use of a series of panels known as the Customize Activation Profiles task. Central storage and expanded storage are allocated in contiguous blocks and may be dynamically reconfigured.

The storage allocated to an LP does not include the Hardware Save Area, which allows a S/390 operating system to have a full 31-bit absolute address space. This area is a logical area of central storage that is not addressable by application programs and is used to store the configuration control information.

In order to access PR/SM logon/access the hardware management console and select the options through the pull down menus. LP definitions can be modified using panels to reset, image, and load profiles. The types of information that can be modified fall into eight categories of parameters as follows:

- **Global Reset Profile Definitions**

  Describe such information as the amount of time a CP may be dispatched or whether event driven dispatching should be turned off. It is recommended that the default be selected. The Global Reset Profile Definitions also may be used to control the order in which LPs can be automatically activated.

- **General Definitions**

  Identify the partitions and their mode of operation, and specify whether the Integrated Coupling Migration Facility (ICMF) is supported.

- **Processor Definitions**

  Describe whether the CPs are dedicated or shared, whether the Internal Coupling Facility (ICF) is to be enabled for a CP, the priority of the CPs, and whether a cryptographic coprocessor is to be used.

- **Security Definitions**

  Determine whether or not performance data may be viewed across partitions, whether an LP can read or write to any IOCDS and make dynamic changes, whether control program commands may be entered that affect other LPs, and whether to reserve unshared reconfigurable channel paths for exclusive use.

- **Storage Definitions**

  Identify the amount of central and expanded storage that can be requested by an LP.

- **Load Definitions**

  Identify the IPL address and dynamic configuration information.

- **Cryptographic Coprocessor Definitions**

  Enable the use of cryptographic functions such as public key secure cable, transport controls, and public key algorithm (PKA).

- **S/370 Channel Definitions**

  Provide the hexadecimal address for the S/370 **CHPID** assignment (cannot be used for S/370 **CHPIDs** for 9672 R5 or later models).

To create, reset, change, and load LP definitions, a series of nine panels known as the Customize Activation Profiles task is used. These panels are available from the support element.

The following describes the Hardware Management Console (HMC) panels (formerly referred to as PR/SM panels) and how a processor complex can be controlled:

- **Options Page**

  Used to identify processor running time and to enable event driven dispatching. It is recommended that the option entitled “**Dynamically determined by the system**” be selected. Otherwise an amount between 1-100 milliseconds running time would be required.

- **Partitions Page**

  Used to identify the order in which LPs are to be activated.

- **General Page**

  Used to identify the LP and the operating mode such as ESA/390.

- **Processor Page**

  Used to identify the number of dedicated central processors, shared processors, whether cryptographic coprocessors are used, and whether to enable the use of the asynchronous data mover (ADM).

- **Security Page**

  Controls the distribution of global performance data and cross partition controls.

- **Storage Page**

  Used to determine in megabytes the amount of initial storage to be used by an LP.

- **Load Page**

  Identifies the IPL address and whether or not automatic activation should occur.

- **Cryptographic Coprocessor Page**

  Used to control cryptographic functions.

- **S/370 Channel Page**

  Identifies the 2-digit hexadecimal address for the S/370 **CHPID** assignment.

- *All access and control of the above panels and the console will be restricted to systems personnel and authorized users.*
- *The Hardware Management Console will not all unauthorized command entry.*

In addition to controlling the processors and the logical partitions using PR/SM parameters and panels, four operator commands can be used to reconfigure a Central Processor Complex. The areas affected are CPs, central storage, and expanded storage. Use the following commands:

- **CF CPU(x),<OFFLINE/ONLINE>**

  This command is used to reconfigure a logical CP on-line or off-line, where **x** is the number of the CP.

- **CF STOR(E=1),<OFFLINE/ONLINE>**

  This command is used to reconfigure a central storage element either on-line or off-line.

- **CF STOR(nnM),<OFFLINE/ONLINE>**

  This command is used to reconfigure smaller amounts of central storage.

- **CF ESTOR(E=x),<OFFLINE/ONLINE>**

  This command is used to reconfigure expanded storage.

NOTE: *The above commands will be ACP protected so that only authorized personnel are able to enter these commands.*

3. MACHINE-SPECIFIC PARTITIONING INFORMATION

3.1 Amdahl

While IBM and Hitachi Data Systems utilize only one IOCDS for the I/O definition, Amdahl machines are able to utilize two IOCDSs. Amdahl Millennium processors use one IOCDS to support the first 256 channels, and a second one to support the second set of 256 channels. Generation of the IOCDS is done using HCD and is activated as part of a domain activation. (Refer to *Section 2.2.1.3, Hardware Configuration Definition (HCD) Program*.)

Multiple Domain Facility (MDF), which functions like PR/SM, defines domains. Specifying the operational characteristics of the domain, which involves allocating the logical resources to include the following, does this:

Logical Processor (LP)
Processor allocations (CPU time)
Storage allocation (main and, optionally, expanded)
IOCDSs
Channels

The definition is then saved to the internal disk of the processor complex. Once the domain is configured and it is activated, normal processing occurs. The activation process actually maps the logical resources in the domain to the actual hardware components.

3.2 Hitachi Data Systems

When working with a Hitachi system, the process is similar to the IBM method. If multiple physical partitions exist, an IOCDS will be required for each partition. If only one physical partition exists, only one IOCDS is used for the entire environment.

The I/O configuration for a Hitachi system is generated in much the same way as for the IBM processors. The IOCDS is created using HCD.

When configuring a Hitachi processor for running logical partitioning, the first requirement is to create an entry for the hardware definition. This is done by creating or modifying the IODF and regenerating the IOCDS.

3.2.1 HCD

When using the HCD method of hardware configuration on a Hitachi system, complete the following steps:

(1) When using HCD, create the new IODF or modify an existing one using the panels provided. Upon completion of the changes, activate the IODF and load the updated hardware and software changes.

(2) The HCD may either be implemented using a POR, or with Dynamic I/O Reconfiguration as indicated in the following paragraphs:

(a) If using the POR method, this is performed in the same manner as if using an IOCDS. After the SYSIML, the IODF is specified using the LOAD entry on the OPRCTL screen. The information included contains the IODF volume, the suffix of the IODF, and the I/O suffix from **SYS1.NUCLEUS**.

(b) If the new configuration is done completely within HCD, the production IODF is made active by issuing the **ACTIVATE** command.

(c) If not using dynamic reconfiguration, the production IODF may be specified at IPL time by using the **PARM** parameter under the LOAD entry on the OPRCTL screen. The information included contains the IODF volume, the suffix of the production IODF, and the I/O suffix from **SYS1.NUCLEUS**.

NOTE: *Refer to Section 2.2.1.3, Hardware Configuration Definition (HCD) Program.*

3.3 IBM

IBM processors may be configured for physical partitioning. Do this by dividing the hardware into logical partitions (LPs). Each logical partition (LP) is configured to run one operating system. Thus, the hardware can run more than one operating system by having more than one LP.

When configuring an IBM processor for running logical partitioning, the first requirement is to create an entry for the hardware definition. Creating or modifying an IOCDS entry or an IODF does this. Some CMOS processors are unable to be divided into multiple LPARs because of a lack of resources.

3.3.1 HCD

When using HCD to create a hardware configuration on an IBM system, complete the following steps:

(1) Create the new work IODF or modify an existing one using the HCD panels provided. Upon completion of the changes, activate the IODF and load the updated hardware and software changes.

(2) The production IODF may either be implemented using a POR, or with Dynamic I/O Reconfiguration as indicated in the following paragraphs:

(a) If using the POR method, this is performed in the same manner as if using an IOCDS. After the POR, the IODF is specified using the LOAD entry on the OPRCTL screen. The information included contains the IODF volume, the suffix of the IODF, and the I/O suffix from **SYS1.NUCLEUS**.

(b) If the new configuration is done completely within HCD, the production IODF is made active by issuing the **ACTIVATE** command.

(c) If not using dynamic reconfiguration, the production IODF may be specified at IPL time by using the **PARM** parameter under the LOAD entry on the OPRCTL screen. The information included contains the production IODF volume, the suffix of the production IODF, and the I/O suffix from **SYS1.NUCLEUS**.

NOTE: *Refer to Section 2.2.1.3, Hardware Configuration Definition (HCD) Program. For VM LPARs, the IOCP utility program can perform the same function as HCD.*

- *The IAO will ensure that the LOADxx members are named in accordance with DISA standards and follow the guidelines specified in DISA Computing Service's Naming Convention Standards handbook.*

This page is intentionally left blank.

4. LPAR SECURITY

4.1 General LPAR Security Issues

The number of sites supplying IBM or IBM-compatible processors has decreased. This has made it necessary to increase the number of domains. This involves configuring a processor to concurrently run more than one instance of an operating system.

When this is done, many factors must be taken into account. These include security classification, the LPAR test or production level of service requirements (e.g., 24 x 7, etc.), and availability of resources.

4.1.1 Introduction to General LPAR Security Considerations

The first security issue to be evaluated in a logical partitioning environment involves the tools that create the LPAR in the first place. These fall into the following two groups:

Programs that create the LPAR
Input files containing the control statements used to generate the different LPARs

The programs include HCD, MVSCP, and the appropriate *****IOCP** program. These programs will be excluded from all but those who are responsible for maintaining the IOCDS and the MVSCP.

The source input required to create or make changes to the LPAR will also be adequately protected. The data sets containing the source should be unavailable to all but the systems programmers. In most cases, only systems programmers need to be aware that these files exist at all. This is true regardless of the classification of the LPAR.

4.2 LPAR Security by Classification Environment

In this section the security requirements are discussed based on the specifics of the particular environment. It must be noted that the requirements for a particular environment are always based on the **highest** classification to be used in that environment. In other words, if **Secret** is the highest classified partition being executed, then the environment in that room will be treated as **Secret**, and all personnel working in that room will have at least a **Secret** security clearance.

Additionally, the controls for a specific processor complex will be based on the highest level of processing occurring on the complex. As an example, if a processor complex runs both test and production LPARs, the rules for production environments will apply.

4.2.1 Test Environment Requirements

This environment requires the lowest level of security. If no LPARs exist other than for testing, this environment may be used for the processor complex.

NOTE: *A test environment will be defined according to the OS/390 STIG, Section 1.9.3, Development and Test Domains.*

4.2.1.1 DISA Physical Requirements for the Test LPAR Environment

Apply the following physical security requirements to the physical processor and LPAR:

(1) House the physical processor complex in a secured facility. The site Operations management will grant access to those who have a need to be in the facility. This will be determined based upon job requirements and in accordance with the *COMPUTING SERVICES Security Handbook.*

(2) Locate both the system console attached to the service processor and the operating system (MVS) console within the confines of the secured facility. A secured facility is one where access is controlled, the computer room is locked, and admittance is permitted to only Operations and Systems personnel.

(3) Some processor complexes support the use of PCs for performing remote service console functions (e.g., EX/CF on Hitachi systems). Only implement this on processor complexes that are **not** processing any classified data. In addition, if any consoles are located in an unsecured area, they will be locked at all times when not in use.

- *The IAO will ensure that that Hardware Management Console is located in a controlled area and access to the Hardware Management Console is restricted to authorized personnel.*
- *The IAO will ensure that micro-code updates to the Hardware Management Console are tracked.*

4.2.1.2 DISA Maintenance Requirements for the Test LPAR Environment

Apply the following requirements to the maintenance of the microcode controlling the processor complex in a test environment:

(1) Permit automatic dial-out to the vendor for diagnostic purposes only on complexes containing no classified data or partitions.

(2) The Field Engineer will not apply microcode maintenance and/or upgrades without the prior knowledge and authorization of site Operations management.

(3) Ensure that vendor personnel are cleared to the level of the highest classification being processed in the processor complex.

(4) The site Systems and Security staffs will review all maintenance actions in advance to assess their impact. Track revision levels for microcode components to ensure that the reviews have been done. **Alpha** and **beta** microcode maintenance may be installed and tested for fitness of use.

4.2.1.3 DISA Resources for the Test LPAR Environment

Apply the following requirements to test LPAR-level resources:

(1) **I/O Configuration and Channels:**

(a) To prevent an unauthorized update of the IOCDS for the physical processor or partition, protect the IOCP input and the appropriate processing programs (e.g., IOPIOCP, HCD, etc.) using the standard features of the resident ACP. Protect the processing programs as sensitive utilities. Depending on how the site manages its *sysgens*, the LPRCTL frame may be used as a supplemental security mechanism.

(b) Channel paths within a test LPAR environment may be defined to the partition as reconfigurable.

(c) The test LPAR may be marked as reconfigurable within the system management (e.g., MLPF) partitioning screens.

(2) **Storage:**

(a) The storage within a test partition may be reconfigurable.

(b) The storage may be reconfigured using control commands such as **MVSTOR**, and may be used within the test environment.

(3) **Processors:**

Processors may be shared or allocated physically or logically within the test environment.

(4) **DASD:**

(a) DASD devices may be shared as necessary when working in the test environment.

(b) Solid State DASD may be shared in the same manner when necessary.

(5) **Tape Units:**

Tape devices may be shared when working in a test environment and may be available to either environment if necessary.

(6) **Printers:**

Printers may be allocated to any LPAR on an as-needed basis. Switching units or patch boards may also be used.

4.2.1.4 DISA Communications Resources for the Test LPAR Environment

Apply the following requirements to the communications configuration of, and user access to, the LPAR:

(1) **Communications:**

(a) Access to the LPAR may be from on-site at the site, or from off-site at remote office locations as required.

(b) Dial-up access and LAN connectivity to the LPAR, access to the Internet, and mail server access are permitted.

(2) **General Users:**

Users may access the LPAR from on-site or remote office locations.

4.2.2 Production Environment Requirements

4.2.2.1 DISA Physical Requirements for the Production LPAR Environment

Apply the following physical security requirements to the physical processor and LPAR:

(1) House the physical processor complex in a secured facility. At a minimum, rate the facility in accordance with the *COMPUTING SERVICES Security Handbook.*

(2) Locate both the system console attached to the service processor and the operating system (OS/390) console within the confines of the secured facility. Ensure that all personnel accessing the facility have the necessary clearances, whether or not they directly contact the production system.

(3) Some processor complexes support the use of PCs for performing remote system console functions (e.g., EX/CF on Hitachi systems). This may be implemented at the discretion of the site if the feature is used solely within the confines of data center operations, and the PC is physically secured in the same fashion as the system console.

(1) Ensure that dial-up access to the service console is disabled during normal operations. If required, it may be enabled temporarily for vendor support.

- *The IAO will ensure that that Hardware Management Console is located in a controlled area and access to the Hardware Management Console is restricted to authorized personnel.*

- *The IAO will ensure that micro-code updates to the Hardware Management Console are tracked.*
- *Unauthorized alternate Hardware Management Console will not be used.*
- *The Hardware Management Console event log will be used to record system events.*

4.2.2.2 DISA Maintenance Requirements for the Production LPAR Environment

Apply the following requirements to the maintenance of the microcode controlling the processor complex in a production environment:

(1) If the processor complex supports automatic dial-out to the vendor for diagnostic purposes in the event a problem is detected, use of this feature is permissible.

(2) Ensure that vendor personnel are cleared to the level of the highest classification being processed in the processor complex.

(3) The site Systems and Security staffs will review all maintenance actions in advance to assess their impact. Track revision levels for microcode components to ensure that the reviews have been done. Only install maintenance that is not **Generally Available** (in **GA** status) in emergencies. Only in emergencies will **alpha** or **beta** testing of microcode changes be done on processor complexes supporting production environments.

4.2.2.3 DISA Resources for the Production LPAR Environment

Apply the following requirements to production LPAR-level resources:

(1) **I/O Configuration and Channels:**

(a) To prevent an unauthorized update of the IOCDS for the physical processor or the partition, protect the IOCP input and the appropriate processing programs (e.g., IOPIOCP, HCD, etc.) using the standard features of the resident ACP. Protect the processing programs as sensitive utilities. Depending on how the site manages its *sysgens*, the LPRCTL frame may be used as a supplemental security mechanism.

(b) Channel paths defined to a production partition may be defined in the IOCDS as reconfigurable.

(c) The production LPAR may be reconfigurable.

(d) Channel-switching units or patch boards may be used to control the channels assigned to the LPAR.

(2) **Storage:**

(a) Mark all storage defined to the partition as non-reconfigurable (for classified processing) within the system management (e.g., MLPF) partitioning screens.

(b) Storage control commands may be used to reconfigure frames as required, and will conform to requirements in the *COMPUTING SERVICES Security Handbook*.

(c) Expanded storage poses no risk, and may be used at the discretion of the site.

(3) **Processors:**

Physical and logical processors may be partitioned as required in the production environment.

(4) **DASD:**

Dedicate DASD devices to the LPAR at the control-unit level. A control unit may manage DASD on a production LPAR and may be shared as required (**provided the necessary ACP rules are in effect**).

(5) **Tape Units:**

(a) Allocate tape devices to the LPAR at the Tape Control Unit (TCU) level. A TCU may concurrently manage tape drives on multiple production LPARs.

(b) Tape Silo units may be shared within production LPARs at the control-unit level.

(6) **Printers:**

Allocate printers from production LPAR to production LPAR on an as-needed basis.

4.2.2.4 DISA Communications Resources for the Production LPAR Environment

Apply the following requirements to the communications configuration of, and user access to, the production LPAR environment:

(1) **Communications:**

(a) Share all communications devices (e.g., FEPs or FEP partitions) to the LPAR.

(b) Access to the LPAR may be from on-site at the site, or from off-site at remote office locations. Connect all terminals to the LPAR using the appropriate protocol in accordance with the current *Network Infrastructure STIG*.

(2) **General Users:**

General users may access the LPAR from on-site or remote office locations.

(3) **Privileged Users (Systems Programmers, Application Systems Maintenance Personnel, etc.):**

Only allow access for privileged users from on-site terminals on locally attached control units, or when using SecurID extended user authentication cards and the CSF software product to log on to the LPAR.

4.2.2.5 DISA Additional Production System Resource Requirements

Apply the following additional system requirements to the LPAR:

(1) Retain all system output (e.g., SMF data, SYSLOG, System Logrec data, ACP log files, etc.) to ensure the availability of an audit trail of system activity for one year.

Refer to the *OS/390 STIG, Section 2.1.2.10, SMF Data Collection, Section 3.1.2, Userid Controls*, and *Section 3.3.1, Standard Global Options (SETROPTS)*, for further information.

(2) The resident ACP will discretely control all access to data. Grant access strictly on a **need-to-know** basis.

4.2.3 Classified Environment Requirements

4.2.3.1 DISA Physical Requirements for the Classified LPAR Environment

Apply the following physical security requirements to the physical processor and LPAR when running a classified environment:

(1) House the physical processor complex in a secured facility. At a minimum, rate the facility as **Approved for Collateral Storage** for **Secret** in accordance with the *COMPUTING SERVICES Security Handbook.*

(2) Locate both the system console attached to the service processor and the operating system (MVS) console within the confines of the secured facility. Ensure that all personnel accessing the facility have the appropriate clearances, whether or not they directly contact the classified system.

(3) Some processor complexes support the use of PCs for performing remote system console functions (e.g., EX/CF on Hitachi systems). This may be implemented at the discretion of the site if the feature is used solely within the confines of data center operations, and the PC is physically secured in the same fashion as the system console.

(2) Disable dial-up access to the system console.

- *The IAO will maintain written procedures for handling the introduction of classified information into the system.*

- *The IAO will ensure that automatic dial-out access to the Hardware Management Console is not activated for classified LPARs.*
- *The IAO will ensure that the automatic dial-in facility is restricted for classified LPARs.*
- *All channel paths for classified LPARs will be restricted to the classified processor.*
- *The Global Performance Data Control option* ***will*** *be turned off for classified LPARs.*
- *The Dedicated Central Processors option* ***must*** *be turned on for classified LPARs on shared sysplexes.*

4.2.3.2 DISA Maintenance Requirements for the Classified LPAR Environment

Apply the following requirements to the maintenance of the microcode controlling the processor complex:

(1) If the processor complex supports automatic dial-out to the vendor for diagnostic purposes in the event a problem is detected, use of this feature will be permissible only if STU-III devices are used to secure the communications link. Otherwise, disable this feature.

(2) Ensure that vendor personnel are cleared to the level of the highest classification being processed in the processor complex.

(3) The site Systems and Security staffs will review all maintenance actions in advance to assess their impact. Track revision levels for microcode components to ensure that the reviews have been done. Only install maintenance that is **Generally Available** (in **GA** status) in emergencies. **Alpha** or **beta** testing of microcode changes will **not** be done in a DISA environment.

- *The IAO will ensure that the automatic dial-in facility for classified LPARs is restricted.*

4.2.3.3 DISA Resources for the Classified LPAR Environment

Apply the following requirements to classified LPAR-level resources:

(1) **I/O Configuration and Channels:**

(a) To prevent an unauthorized update of the IOCDS for the physical processor or partition housing the classified LPAR, protect the IOCP input and the appropriate processing programs (e.g., IOPIOCP, HCD, etc.) using the standard features of the resident ACP. Protect the processing programs as sensitive utilities. Depending on how the site manages its *sysgens*, the LPRCTL frame may be used as a supplemental security mechanism.

(b) Some processor complexes (e.g., Amdahl processors that use MDF) utilize one IOCDS for each domain, as opposed to one for each physical partition, and allow the dynamic reconfiguration of channels between domains. When implementing a classified domain on such a processor, implement procedures to ensure that channels are not dynamically reconfigured from the classified domain to any other domain.

(c) Define all channel paths that are defined to the partition in the IOCDS as dedicated.

(d) Mark the classified LPAR as non-reconfigurable within the system management (e.g., MLPF) partitioning screens.

(e) To avoid inadvertent device misallocation, define the system generation (e.g., *sysgen*, MVS/CP GEN, HCD, etc.) for each LPAR on the physical processor complex with only those devices associated with the system executing in the LPAR.

(f) Do **not** use channel-switching units or patch boards to control the channels assigned to the LPAR.

(2) **Storage:**

(a) Mark all storage defined to the partition as non-reconfigurable within the system management (e.g., MLPF) partitioning screens.

(b) Operations IPL procedures will explicitly state that from the IPL screen, either separate Clear Storage and Load commands are both done, or the Clear/Load command is issued. Never perform the Load without a Clear Storage first. The only exception to this is when a Stand Alone Dump (SAD) is performed at the request of the systems programming staff. In this case, the Load must be done without the Clear, or the diagnostic data will be unavailable. Also in this case, the SAD tape will be handled in a secure fashion, as will any output produced by systems programming personnel using the **dump** facility.

(c) Do not use the **MVSTOR** command for the movement of the classified LPAR’s frames, since a risk is introduced in the event of a microcode error.

(d) Expanded storage poses no risk and may be used at the discretion of the site.

(e) Do not configure expanded storage off-line from the classified LPAR, and then on-line to another LPAR, unless a POR is done to clear the contents of the storage.

(3) **Processors:**

Mixing classified and unclassified LPARs on a single host requires the approval of the National Security Agency (NSA). At this time, NSA has not approved any such mix. Therefore, classified and unclassified LPARs are not permitted on the same host.

NOTE: *Currently, there are no TEST Classified LPARs at any of the Sites, and there are no plans for any to be created. If a requirement for the creation of a TEST Classified LPAR comes up in the future, the same requirements apply to the TEST Classified LPARs as for the Production Classified LPARs.*

(4) **DASD:**

(a) Dedicate DASD devices to the LPAR at the control-unit level. A control unit will not manage DASD on both the classified LPAR and another LPAR. All DASD on a dedicated string will be accessible only from that single LPAR. These restrictions also extend to all DASD housing system volumes and data.

(b) Do not cross-cable DASD units to control units on both the classified LPAR and another LPAR.

(c) Dedicate Solid State DASD units to the LPAR at the control-unit level. The entire Solid State unit will be dedicated to the classified LPAR and unavailable to any other LPAR.

(d) Dedicate RAID units to the LPAR at the control-unit level. The entire RAID unit will be dedicated to the classified LPAR and unavailable to any other LPAR.

(5) **Tape Units:**

(a) Allocate tape devices to the LPAR at the Tape Control Unit (TCU) level. A TCU will not concurrently manage tape drives on both the classified LPAR and another LPAR. Also, all tape drives on the allocated string will be accessible only from that single LPAR.

(b) Tape devices may be allocated to the classified LPAR on an as-needed basis, as long as they are reallocated at the TCU level.

(c) Dedicate Tape Silo units to the LPAR at the control-unit level. The entire Tape Silo unit will be dedicated to the classified LPAR and unavailable to any other LPAR.

(d) Physically segregate the tape library from all other tape libraries to avoid accidental compromise of data. Degauss all tapes that have reached their expiration date before returning them to the tape library for reuse.

(e) To mitigate the risk and ensure that tape volumes are not inadvertently stored or used with the wrong LPAR, the tape volume ranges used on the classified LPAR will be unique, and will not match ranges used on other LPARs housed within the physical facility.

(6) **Printers:**

(a) Printers may be allocated to the classified LPAR on an as-needed basis, as long as they are reallocated at the Interface Control Unit (ICU) level. Switching units or patch boards may also be used to control and assign the individual print devices.

(b) Hard copy output from the classified LPAR will be appropriately marked and handled in a secure fashion. The user will sign for it. When no longer needed, dispose of it in an approved manner (e.g., burned, shredded, etc.).

4.2.3.4 DISA Communications Resources for the Classified LPAR Environment

Apply the following requirements to the communications configuration of, and user access to, the LPAR:

(1) **Communications:**

(a) Dedicate all communications devices (e.g., FEPs or FEP partitions) to the LPAR. Before switching a dedicated FEP partition to another LPAR, clear the partition's internal storage and reload the FEP *gen*.

(b) Access to the LPAR may be from on-site at the site or from off-site at remote office locations. Connect all terminals to the LPAR using the SNA networking protocol or via the SIPRNet.

(c) Secure access to remote SNA terminals using NSA Type I encryption technology (e.g., KG84).

(d) Disallow LAN connectivity to the LPAR except via the SIPRNet or with a physical connection directly to a local LAN that has no other connections.

(e) Disallow access to the Internet including mail access.

(f) Only allow dial-up access to the LPAR if STU-III devices are used to secure the connection.

(2) **General Users:**

(a) General users may access the LPAR from on-site or remote office locations.

(b) It is recommended, but not required at this time, that extended user authentication (e.g., SecurID cards and the CSF software product) be used to verify all users when they log on to the LPAR.

(3) **Privileged Users (Systems Programmers, Application Systems Maintenance Personnel, etc.):**

(a) Only allow access for **privileged** users from on-site terminals on locally attached control units.

(b) These users will be required to use SecurID extended user authentication cards and the CSF software product to log on to the LPAR.

4.2.3.5 DISA Additional Classified System Resource Requirements

Apply the following additional system requirements to the LPAR:

(1) Ensure that the **Erase-on-Delete** feature is activated on the system ACP for all data.

(2) Retain and secure all system output (e.g., SMF data, SYSLOG, System Logrec data, ACP log files, etc.) for one year. The data will be retained in duplicate to ensure the availability of an audit trail of system activity.

Refer to the *OS/390 STIG, Section 2.1.2.10, SMF Data Collection,* for further information.

(3) In the S/390 system running in the classified LPAR, specify the MVS parameter **RSU** in **IEASYS00** with a zero (**0**) value to indicate that no storage is marked as reconfigurable.

(4) The resident ACP will discretely control all access to system and customer data. Access will be granted strictly on a **need-to-know** basis, and the default for all data will be to disallow access. Do not use fall-through rules to grant access.

4.3 Restricted LPAR Environment Requirements

4.3.1 DISA Physical Requirements for the Restricted LPAR Environment

Apply the following physical security requirements to the physical processor and LPAR when running a restricted environment:

(1) House the physical processor complex in a secured facility. At a minimum, rate the facility as **Approved for Collateral Storage** for **Secret** in accordance with the *COMPUTING SERVICES Security Handbook.*

(2) Locate both the system console attached to the service processor and the operating system (MVS) console within the confines of the secured facility. Ensure that all personnel accessing the facility have the appropriate clearances, whether or not they directly contact the restricted system.

(3) Some processor complexes support the use of PCs for performing remote system console functions (e.g., EX/CF on Hitachi systems). This may be implemented at the discretion of the site if the feature is used solely within the confines of data center operations, and the PC is physically secured in the same fashion as the system console.

(3) Disable dial-up access to the system console.

- *The IAO will maintain written procedures for handling the introduction of restricted information into the system.*
- *The IAO will ensure that automatic dial-out access to the Hardware Management Console is not activated for restricted LPARs.*
- *The IAO will ensure that the automatic dial-in facility is restricted for restricted LPARs.*
- *All channel paths for restricted LPARs will be restricted to the restricted processor.*
- *The Global Performance Data Control option* ***will*** *be turned off for restricted LPARs.*
- *The Dedicated Central Processors option* ***must*** *be turned on for restricted LPARs on shared sysplexes.*

4.3.2 DISA Maintenance Requirements for the Restricted LPAR Environment

Apply the following requirements to the maintenance of the microcode controlling the processor complex:

(1) If the processor complex supports automatic dial-out to the vendor for diagnostic purposes in the event a problem is detected, use of this feature will be permissible only if STU-III devices are used to secure the communications link. Otherwise, disable this feature.

(2) Ensure that vendor personnel are cleared to the level of the highest classification being processed in the processor complex.

(4) The site Systems and Security staffs will review all maintenance actions in advance to assess their impact. Track revision levels for microcode components to ensure that the reviews have been done. Only install maintenance that is **Generally Available** (in **GA** status) in emergencies. **Alpha** or **beta** testing of microcode changes will **not** be done in a DISA environment.

- *The IAO will ensure that the automatic dial-in facility for restricted LPARs is restricted.*

4.3.3 DISA Resources for the Restricted LPAR Environment

Apply the following requirements to restricted LPAR-level resources:

(1) **I/O Configuration and Channels:**

(a) To prevent an unauthorized update of the IOCDS for the physical processor or partition housing the restricted LPAR, protect the IOCP input and the appropriate processing programs (e.g., IOPIOCP, HCD, etc.) using the standard features of the resident ACP. Protect the processing programs as sensitive utilities. Depending on how the site manages its *sysgens*, the LPRCTL frame may be used as a supplemental security mechanism.

(b) Some processor complexes (e.g., Amdahl processors that use MDF) utilize one IOCDS for each domain, as opposed to one for each physical partition, and allow the dynamic reconfiguration of channels between domains. When implementing a restricted domain on such a processor, implement procedures to ensure that channels are not dynamically reconfigured from the restricted domain to any other domain.

(c) Define all channel paths that are defined to the partition in the IOCDS as dedicated.

(d) Mark the restricted LPAR as non-reconfigurable within the system management (e.g., MLPF) partitioning screens.

(e) To avoid inadvertent device misallocation, define the system generation (e.g., *sysgen*, MVS/CP GEN, HCD, etc.) for each LPAR on the physical processor complex with only those devices associated with the system executing in the LPAR.

(f) Do **not** use channel-switching units or patch boards to control the channels assigned to the LPAR.

(2) **Storage:**

(a) Mark all storage defined to the partition as non-reconfigurable within the system management (e.g., MLPF) partitioning screens.

(b) Operations IPL procedures will explicitly state that from the IPL screen, either separate Clear Storage and Load commands are both done, or the Clear/Load command is issued. Never perform the Load without Clear Storage first. The only exception to this is when a Stand Alone Dump (SAD) is performed at the request of the systems programming staff. In this case, the Load must be done without the Clear, or the diagnostic data will be unavailable. Also in this case, the SAD tape will be handled in a secure fashion, as will any output produced by systems programming personnel using the **dump** facility.

(c) Do not use the **MVSTOR** command for the movement of the restricted LPAR’s frames, since a risk is introduced in the event of a microcode error.

(d) Expanded storage poses no risk and may be used at the discretion of the site.

(e) Do not configure expanded storage off-line from the restricted LPAR, and then on-line to another LPAR, unless a POR is done to clear the contents of the storage.

(3) **Processors:**

Mixing restricted and unrestricted LPARs on a single host requires the approval of the National Security Agency (NSA). At this time, NSA has not approved any such mix. Therefore, restricted and unrestricted LPARs are not permitted on the same host.

NOTE: *Currently, there are no TEST Restricted LPARs at any of the Sites, and there are no plans for any to be created. If a requirement for the creation of a TEST Restricted LPAR comes up in the future, the same requirements apply to the TEST Restricted LPARs as for the Production Restricted LPARs.*

(4) **DASD:**

(a) Dedicate DASD devices to the LPAR at the control-unit level. A control unit will not manage DASD on both the restricted LPAR and another LPAR. All DASD on a dedicated string will be accessible only from that single LPAR. These restrictions also extend to all DASD housing system volumes and data.

(b) Do not cross-cable DASD units to control units on both the restricted LPAR and another LPAR.

(c) Dedicate Solid State DASD units to the LPAR at the control-unit level. The entire Solid State unit will be dedicated to the restricted LPAR and unavailable to any other LPAR.

(d) Dedicate RAID units to the LPAR at the control-unit level. The entire RAID unit will be dedicated to the restricted LPAR and unavailable to any other LPAR.

(5) **Tape Units:**

(a) Allocate tape devices to the LPAR at the Tape Control Unit (TCU) level. A TCU will not concurrently manage tape drives on both the restricted LPAR and another LPAR. Also, all tape drives on the allocated string will be accessible only from that single LPAR.

(b) Tape devices may be allocated to the restricted LPAR on an as-needed basis, as long as they are reallocated at the TCU level.

(c) Dedicate Tape Silo units to the LPAR at the control-unit level. The entire Tape Silo unit will be dedicated to the restricted LPAR and unavailable to any other LPAR.

(d) Physically segregate the tape library from all other tape libraries to avoid accidental compromise of data. Degauss all tapes that have reached their expiration date before returning them to the tape library for reuse.

(e) To mitigate the risk and ensure that tape volumes are not inadvertently stored or used with the wrong LPAR, the tape volume ranges used on the restricted LPAR will be unique, and will not match ranges used on other LPARs housed within the physical facility.

(6) **Printers:**

(a) Printers may be allocated to the restricted LPAR on an as-needed basis, as long as they are reallocated at the Interface Control Unit (ICU) level. Switching units or patch boards may also be used to control and assign the individual print devices.

(b) Hard copy output from the restricted LPAR will be appropriately marked and handled in a secure fashion. The user will sign for it. When no longer needed, dispose of it in an approved manner (e.g., burned, shredded, etc.).

4.3.4 DISA Communications Resources for the Restricted LPAR Environment

Apply the following requirements to the communications configuration of, and user access to, the LPAR:

(1) **Communications:**

(a) Dedicate all communications devices (e.g., FEPs or FEP partitions) to the LPAR. Before switching a dedicated FEP partition to another LPAR, clear the partition’s internal storage and reload the FEP *gen*.

(b) Access to the LPAR may be from on-site at the site or from off-site at remote office locations. Connect all terminals to the LPAR using the SNA networking protocol or via the SIPRNet.

(c) Secure access to remote SNA terminals using NSA Type I encryption technology (e.g., KG84).

(d) Disallow LAN connectivity to the LPAR except via the SIPRNet or with a physical connection directly to a local LAN that has no other connections.

(e) Disallow access to the Internet including mail access.

(f) Only allow dial-up access to the LPAR if STU-III devices are used to secure the connection.

(2) **General Users:**

(a) General users may access the LPAR from on-site or remote office locations.

(b) It is recommended, but not required at this time, that extended user authentication (e.g., SecurID cards and the CSF software product) be used to verify all users when they log on to the LPAR.

(3) **Privileged Users (Systems Programmers, Application Systems Maintenance Personnel, etc.):**

(a) Only allow access for **privileged** users from on-site terminals on locally attached control units.

(b) These users will be required to use SecurID extended user authentication cards and the CSF software product to log on to the LPAR.

4.3.5 DISA Additional Restricted System Resource Requirements

Apply the following additional system requirements to the LPAR:

(1) Ensure that the **Erase-on-Delete** feature is activated on the system ACP for all data.

(2) Retain and secure all system output (e.g., SMF data, SYSLOG, System Logrec data, ACP log files, etc.) for one year. The data will be retained in duplicate to ensure the availability of an audit trail of system activity.

Refer to the *OS/390 STIG, Section 2.1.2.10, SMF Data Collection,* for further information.

(3) In the S/390 system running in the restricted LPAR, specify the MVS parameter **RSU** in **IEASYS00** with a zero (**0**) value to indicate that no storage is marked as reconfigurable.

(5) The resident ACP will discretely control all access to system and customer data. Access will be granted strictly on a **need-to-know** basis, and the default for all data will be to disallow access. Do not use fall-through rules to grant access.

4.4 Control Requirements and Disaster Recovery

Refer to the *OS/390 STIG, Section 2.3, Control Requirements*, for information on data set integrity, file location and backup, and file recovery.

This page is intentionally left blank.

5. ENTERPRISE SYSTEM CONNECTION ENVIRONMENT (ESCON)

Vendor: IBM Corporation

5.1 General Considerations

To efficiently manage the transfer of data between processors and devices on S/390 sysplexes, IBM has developed the Enterprise System Connection Environment (ESCON). Through the use of specially designed hardware and software, ESCON eliminates the processor's need to worry about I/O, thus freeing up processors to perform other necessary functions. ESCON is able to improve the transfer rates of data by performing dynamic connectivity. Dynamic connectivity allows a dynamic switch to connect two ports only for the time needed for data transfer. Each port can then be connected to another port on the switch to form another path. In addition, ESCON requires fewer physical interfaces to manage the switching of both sharable and non-sharable devices to other systems, thus affecting overall data center size.

An ESCON environment includes the combination of the hardware and software components discussed in the following sections.

5.1.1 ESCON Channels

ESCON channels are fiber optic channels. Fiber optic cable enables a system to move more data per second compared to parallel copper cable, which is used by earlier machines. Up to 17 million bytes per second can be moved by ESCON for some ES/9000 processor models.

Information transfer through an optical fiber usually occurs in only one direction by using a transmitter and a receiver. The transmitter accepts encoded digital information, converts it into an optical (light) signal, and sends it through the fiber. The receiver detects the optical signal, converts it into an electrical signal, and amplifies it. After being decoded, the digital output information is the same as the digital input. Fiber optic information transfer can also occur in opposite directions simultaneously. This requires the use of two filaments in one fiber optic cable and combines the transmitter, receiver, and duplex receptacle functions into one transmitter-receiver subassembly in each device. Devices directly attached to the processors in a data center no longer need to be within close range. Fiber optic links in conjunction with ESCON directors allow channel-to-channel ranges to be extended.

In order for data to be transferred, it must be broken into frames. Each frame provides the destination, source, control information, and user data. The architecture defines the format of the frame and the rules for the exchange of the data between the channel and the control unit. Once a physical path exists on this interface, all I/O operations are carried out.

5.1.2 ESCON Directors

The primary function of an ESCON Director is to dynamically switch paths between devices so as to ensure channel data rate speeds. Data can flow in each model through all paths at the same time.

An ESCON Director can interconnect any two links attached to any of its ports, providing an enterprise allows them to be connected. An ESCON link consists of all the optical components that provide an information transfer path between two devices. A port can be connected to only one other port at a time, but multiple connections can exist simultaneously. The interconnection of two ports does not affect the ability of the Director to make connections between other pairs of ports. Also, it does not affect the previously existing connections between other port pairs. When the Director establishes a connection, the two ports and their respective point-to-point links are interconnected so that the two links appear as one continuous link for the duration of the connection. When a frame arrives at a port, the Director forwards it through the outgoing port on the link associated with the destination. ESCON Director connections do not have to be dynamic, but in order to make full use of the benefits of ESCON, it is recommended that they be.

When an ESCON Director is powered on, the configuration file, named IPL, is used to describe the last active configuration that was created and saved. Each configuration specifies the Director control units to which a channel is attached, a device address for each Director control unit (which is used for exchanging control and configuration information with the processor), and the addresses associated with each control unit and device. An attribute can be defined or modified from the ESCD console or from a host application, such as ESCON Manager. An attribute can be used to block ports, dedicate ports, and prohibit dynamic connections between ports.

ESCON Directors can also participate in using the ESCON multiple image facility. This allows multiple logical partitions to directly share ESCON channels and ESCON channel-to-channel functions and, optionally, the control units and associated I/O devices configured to these channels.

5.1.2.1 ESCON Director Console (ESCD Console)

An ESCD console is used to provide data center personnel with an interface for displaying and changing an ESCON Director's connectivity attributes. It is also used to install, initialize, and service an ESCON Director. An operator uses a series of menus and data entry screens to perform these functions and others. (Other types of functions performed by operators are password assignments and maintenance. A separate set of menus is also provided so that a vendor service representative can run diagnostics and retrieve log information.)

After making connectivity changes from the ESCD console, a systems programmer can save the configuration for later use or activate it immediately. Even though a maximum of 16 configuration files (including the IPL file) can be saved on the ESCD console fixed disk, it is not recommended. The current configuration and a backup should be stored on the ESCD console fixed disk. A backup should be created on a regular normal cycle and stored for recovery. The configurations, which reside on the fixed disk, can be activated from the ESCD console. They can also be read, written, and deleted by a host program.

The ESCON Director maintains an audit trail at the ESCD console's fixed disk. This audit trail logs the time, date, and password identification when changes have been made to the ESCON Director. The ESCON Director audit trail does not record changes made to the ESCON Director from a host control program. Also, a host control program cannot access the ESCON Director audit trail.

- *The ESCON Director Application Console will be located in a controlled area.*
- *Access to the ESCON Director Application Console will be restricted to authorized personnel.*
- *The ESCON Director Application Console Event log will be enabled.*

5.1.3 ESCON Manager

An ESCON Manager (Enterprise Systems Connection Manager) enables a host to control and manage ESCON Directors defined to the system image. It provides a host with the ability to create dynamic switch configurations in advance and store them for later activation. The ESCON Manager keeps a current view of the host's I/O configuration. The ESCON Manager is able to keep a current configuration by dynamically updating the information about each switch and the actual configuration as the switch and host configurations change. Configuration data activated at a switch controls the potential paths through that switch.

The ESCON Manager's base program executes as an application, which is started and stopped at the system console of the system on which it is running. Commands may be entered through the system's console that could instruct the ESCON Manager to change one or multiple switches in the configuration. Starting or stopping an ESCON Manager base program must be done at the system, or master, console of the host operating system image on which the base program is running.

Whenever a command is entered involving a change to a switch, the ESCON Manager sends the command to the switch to change the configuration data, thus changing potential paths to or through the switch. If an ESCON Manager is unable to successfully perform a function, it will automatically use a **backout** operation so as to ensure that the paths remain on-line. This ensures minimal system interruption during configuration changes. The ESCON Manager can also be used to configure channel paths on-line or offline to a host, and coordinate connectivity changes across multiple hosts, providing the program is running on those hosts and they can communicate with each other through intersystem communication. The application program interface should be restricted to authorized programs.

The ESCON Manager is able to use existing security products that conform to the System Authorization Facility (SAF) to define different levels of authorization for ESCON Manager commands. Therefore, ESCON Manager commands can be differentiated by users and categories. There are three groups of ESCON Manager commands—data display commands, connectivity commands, and utility commands. Since the connectivity and utility commands can change an I/O configuration, they should be restricted to authorized personnel. All ESCON Manager commands, except API-specific commands, can be entered at the system console, sent by the NetView program, or entered through a NetView console.

In order to track changes made to configurations and the commands used to apply the changes, the ESCON Manager uses an audit trail feature. The audit trail feature enables systems personnel to reconstruct and determine the conditions that led up to an error. Use of the audit trail should be standard.

5.1.3.1 ESCON Manager Workstation

The ESCON Manager Workstation feature runs on a programmable workstation that has been enabled for communication with the host image through Advanced Program-to-Program Communications (APPC). The ESCON Manager Workstation provides a Windows like interface. Authorized personnel can obtain graphic views of related objects in the channel subsystem. All of the facilities of the ESCON Manager's API are available through the ESCON Manager Workstation.

The ESCON Manager Workstation provides a mechanism for logging command results and offers an error message log of the workstation activity. The logging feature should be turned on so as to ensure that it could be used to track changes and assist in recovery.

- *The ESCON Manager Workstation will be located in a controlled area.*
- *Access to the ESCON Manager Workstation will be restricted to authorized personnel.*
- *The ESCON Manager audit log will be enabled.*

5.1.3.2 ESCON Manager Commands

The table below lists ESCON Manager commands, whether the command should be logged, and the recommended user:

Table 1. ESCON MANAGER COMMANDS

COMMAND NAME	*PROFILE NAME*	*AUTHORIZED USERS*	*LOG REQ'D*
Allow	IHV.ALLOW	Systems	Y
Block	IHV.BLOCK	Systems	Y
CHAIN	IHV.CHAIN	Systems	Y
Connect	IHV.CONNECT	Systems	Y
DELete File	IHV.DELETE.FILE	Systems	Y
disconNect	IHV.DISCONNECT	Systems	Y
Display Chp	IHV.CHP	Operations (Sr) Systems	N N
Display Dev	IHV.DEV	Operations (Sr) Systems	N N
Display Host	IHV.HOST	Operations (Sr) Systems	N N
Display Name	IHV.NAME	Operations (Sr) Systems	N N
Display Port	IHV.PORT	Operations (Sr) Systems	N N
Display Results	IHV.RESULTS	Operations (Sr) Systems	N N
Display Switch	IHV.SWITCH	Operations (Sr) Systems	N N
Display Timeout	IHV.TIMEOUT	Operations (Sr) Systems	N N
Display Vary	IHV.VARY	Operations (Sr) Systems	N N
GETLOCK	IHV.GETLOCK	Systems	Y
LOGREC	IHV.LOGREC	Systems	Y
Prohibit	IHV.PROHIBIT	Systems	Y
Query Entity	IHV.QUERY.ENTITY	Operations (Sr) Systems	N N
Query File	IHV.QUERY.FILE	Operations (Sr) Systems	Y Y
Query Interface	IHV.QUERY.INTERFACE	Operations (Sr) Systems	N N
Query Relation	IHV.QUERY.RELATION	Operations (Sr) Systems	Y Y
Query Switch	IHV.QUERY.SWITCH	Operations (Sr) Systems	N N

COMMAND NAME	*PROFILE NAME*	*AUTHORIZED USERS*	*LOG REQ'D*
REMOVE Chp	IHV.REMOVE.CHP	Systems	Y
REMOVE Switch	IHV.REMOVE.SWITCH	Systems	Y
Reset Host	IHV.RESET.HOST	Systems	Y
Reset Switch	IHV.RESET.SWITCH	Systems	Y
Reset Timeout	IHV.RESET.TIMEOUT	Systems	Y
RESTORE Chp	IHV.RESTORE.CHP	Systems	Y
RESTORE Switch	IHV.RESTORE.SWITCH	Systems	Y
SYNC Switch	IHV.SYNC.SWITCH	Systems	Y
Unblock	IHV.UNBLOCK	Systems	Y
UNCHAIN	IHV.UNCHAIN	Systems	Y
UNLOCK	IHV.UNLOCK	Systems	Y
Write	IHV.WRITE	Systems	Y
WRITEFILE	IHV.WRITEFILE	Systems	Y
WRITEPORT	IHV.WRITEPORT	Systems	Y
WRITESWCH	IHV.WRITESWCH	Systems	Y

- *The IAO will ensure that the ESCON Manager Commands are restricted to authorized personnel. The log option will be enabled for all accesses.*

5.2 General Security Considerations

Because ESCON manages the transfer of data between processors and devices on S/390 sysplexes, its control and security must be ensured. By doing so, data integrity can be maintained. The ESCON Manager is used as a tool to manage an ESCON configuration, which generally contains critical I/O resources. Access to the program will need to be restricted in virtually all enterprises. There are multiple layers of ESCON security that can be enabled to minimize unauthorized access. The following security measures should be implemented:

(1) Protect all ESCON system data sets using appropriate ACP data set rules.

(2) Limit access and restrict all ESCON Manager commands to systems programming personnel and specifically authorized personnel as deemed by the site.

(3) Apply password controls for authorized users of the ESCD Console.

(4) Apply userid and password restrictions on access to the ESCM Workstation.

NOTE: *The next two subsections describe the security considerations as they relate to the ESCD Console and the ESCON Workstation Manager.*

- *The* ***Distributed Console Access Facility (DCAF)*** *will be restricted to authorized personnel.*

5.2.1 ESCON Director Console Security (ESCD Console)

The ESCD console and its associated ESCON Director can be secured using passwords. Three levels of password controls have been established. Each password level controls different ESCD console functions. Prior to making any changes or accessing utilities or maintenance procedures, a user is required to enter a password. A password administrator must use the ESCD console to enable an authorized user access. Following are the three levels of password authority:

Administration (Level 1)

Restrict to systems programming personnel who serve as administrators. A Level 1 password allows the user to display, add, change, and delete passwords of all of the ESCON Director Level 1, Level 2, and Level 3 users. It does not allow the administrator to access maintenance procedures or utilities or to change connectivity attributes.

Maintenance (Level 2)

Restrict to service representatives who perform maintenance procedures. Level 2 users cannot view other users' passwords, change passwords, change connectivity attributes, or access utilities.

Operations (Level 3)

Restrict to systems programming personnel who are responsible for changing connectivity attributes and accessing certain utilities. Level 3 users cannot view other users' passwords, change passwords, or perform maintenance procedures.

NOTE: *Passwords are* **not** *required to enter display commands at the ESCD console, to access the audit trail, or to create a backup diskette.*

An ESCON Director allows the password administrator to assign up to 30 users to each password level. Passwords must be at least eight characters in length (reference *DOD Directive 8500.aa, dated September 26, 2001 [draft]*). It is recommended that passwords conform to DISA standards. A password identifier is associated with each password, and the password administrator may enter a user description for each password.

All default passwords should be changed as soon as possible after installing the ESCON Director. When using the Console Sharing option, there is one set of passwords for all ESCON Directors that share the console. Ensure that the set of passwords are restricted to authorized personnel and changed at regular intervals.

5.2.2 ESCON Manager Workstation Security

Userids and passwords are required for authorized personnel to access an ESCON Manager Workstation. Although it is possible for several users at different workstations to communicate with the ESCON Manager base program using the same userid, this is not a recommended practice. It means losing the protection of individual ownership and auditability provided by the ESCON Manager's process locking mechanism.

Power-on passwords help to ensure secure access to the workstation. Before starting a host session to use ESCON Manager commands, the workstation requires a userid and password to be entered, which it sends to the host operating system being addressed for verification. A userid is required for each active host configuration. Not only must the userid and password be defined to the host security program (ACF2, RACF, or TOP SECRET), but it also must have the appropriate level of security assigned in the security database. In order for authorized users to access APPC, a userid must be entered.

5.3 ACF2

Access to the **ESCON MANAGER** facility (used to modify the ESCON Director configurations) will be protected using the ACF2 class restriction. All commands with **IHV.*** prefix should be protected, as described in *Table 1*. Standard data set access rules are required for the library containing the program. The ESCON Manager program for the started task must be in a protected library.

5.4 RACF

Access to the **ESCON MANAGER** facility (used to modify the ESCON Director configurations) will be protected using the **FACILITY** class. All commands with **IHV.*** prefix should be protected, as described in *Table 1*. Standard data set access rules are required for the library containing the program. The ESCON Manager program for the started task must be in a protected library.

5.5 TOP SECRET

Access to the **ESCON MANAGER** facility (used to modify the ESCON Director configurations) will be protected using the TOP SECRET class restriction. All commands with **IHV.*** prefix should be protected, as described in *Table 1*. Standard data set access rules are required for the library containing the program. The ESCON Manager program for the started task must be in a protected library.

6. SYSTEMS COMPLEX SYSPLEX

Vendor: IBM

6.1 General Considerations

A system complex, **sysplex**, is a group of IBM OS/390 or z/OS systems that work together, using certain hardware and software products, to support an installation’s processing needs. Sysplexes are the result of an evolutionary process of large mainframe processing requirements.

Originally, large mainframes consisted of a central processor CP and software to control its processing. S/390 Architecture dictates that a CP executes one program instruction at a time. CPs were combined with channels and storage to form central processor complexes CPCs. One MVS operating system running on a CPC was referred to as a Single System Uniprocessor.

CPCs were configured differently to address processing needs. CPCs were configured as tightly coupled and loosely coupled systems. As a result of adding additional CPs to a CPC, central processor complexes were able to perform simultaneous program instruction processing. Thus the CPC was able to increase processing capabilities. Loosely coupled configurations used channel-to-channel communications that allowed multiple MVS systems to communicate.

In order to solve the problems of managing multiple MVS systems, sysplexes were introduced. Sysplexes are enabling multisystem management through the cross-system coupling facility (XCF) component of MVS/ESA. XCF services allow authorized applications on one system to communicate with applications on the same system or on other systems. Thus, CPCs were able to connect by channel-to-channel communications and share the datasets that support communication. In addition, sysplexes enabled parallel processing. Thus applications were able to better utilize the CPC more efficiently.

When more than one CPC is involved, a Sysplex Timer synchronizes the time on all systems. In order to support a greater number of systems and improve communication, parallel sysplexes were developed. Parallel Sysplexes use the coupling facility to support subsystems such as the Information Management System (IMS) to ensure the integrity and consistency of data in a sysplex. In addition, Parallel Sysplexes use workload management software to manage throughput and Automated Error Recovery to restore processing to down images.

Sysplexes provide parallel capabilities on many levels, in applications, the sysplex software, and the hardware. Between the hardware and software products sysplexes provide for a greater degree of parallelism that enables a more efficient uses of resources.

6.1.1 Sysplex Hardware and Software

As mentioned earlier, Sysplexes use a group of hardware and software facilities to support an installation’ s processing needs. The following hardware and software was designed to support or was enhanced to support sysplexes:

Hardware:

- Coupling Facility
- Coupling Facility Channels
- Sysplex Timers
- System/390 Processors
- ESCON Channels and Directors
- ESCON Control Units and I/O Devices

Software:

- OS/390, z/OS JES2 and JES3, and DFSMS
- Virtual Telecommunications Access Method (VTAM)
- Information Management System Database Manager (IMS DB),
- DATABASE 2 (DB2)
- Virtual Storage Access Method (VSAM).
- Customer Information Control System (CICS/ESA and CICS Transaction Server)
- Information Management System Transaction Manager (IMS TM).
- CICSPlex System Manager/ESA (CICSPlex SM)
- Operations Planning and Control (OPC/ESA)
- Workload Manager (WLM)
- System Automation for OS/390
- Hardware Management Console
- System Display and Search Facility (SDSF)
- Enterprise Performance Data Manager/MVS (EPDM)
- Service Level Reporter (SLR)
- System Automation for OS/390
- Hardware Configuration Definition (HCD)

6.1.2 Enhancements

6.1.2.1 Cross System Coupling (XCF)

The cross-system coupling facility (XCF) component enables authorized programs in a sysplex to communicate with programs on the same MVS system or other MVS systems. XCF services allow multiple instances of an application or subsystem, running on different systems in a sysplex, to share status information and communicate with each other. Section 7.6.1 provides greater detail on XCF.

- *The IAO will ensure that ACP rules exist restricting update access to the XCF data sets.*
- *The IAO will ensure that the facility resource classes are created for XCF.*

6.1.2.2 z/OS or OS/390

z/OS or OS/390 enable new coupling technology to extend system support beyond the previous limit of 8 MVS systems, and increases the number of I/O devices allowed per MVS system beyond the previous limit of 4096. It is the platform for simplified systems management of a sysplex, including configuration management, availability management, workload management, and single-image operations. Additional enhancements include problem determination and recovery in a sysplex.

6.1.2.3 JES2 or JES3

Both job entry subsystem products control job queues and dispatch work in a sysplex. JES2 expands its 7-member multi-access spool (MAS) capability to a 32-member MAS. Additionally, JES2 uses the coupling facility to enhance its performance. JES3 can support a maximum of 32 members in a JES3 complex and supports ESCON CTCs or the coupling facility.

6.1.2.4 DFSMS

DFSMS enables the automatic placement, migration, backup, recall, recovery, and deletion of data for z/OS. An SMS configuration can contain 32 names, but the names can be a combination of system names and system group names. DFSMS also supports the increased number of I/O devices beyond the previous limit of 4096.

6.1.2.5 Virtual Telecommunications Access Method (VTAM)

VTAM monitors and controls the activation and connection of resources in a network. When VTAM is part of the sysplex, duplicate applications on different systems in a VTAM network can identify themselves by a single generic resource name. By distributing sessions among a number of duplicate resources under a single name, instead of to a uniquely named single resource, VTAM is capable of balancing the session workload.

6.1.2.6 Virtual Storage Access Method (VSAM) - component of DFSMS

DFSMS has been enhanced to support a new VSAM data set accessing mode called record level sharing (RLS). VSAM RLS provides sysplex data sharing and will use the coupling facility for locking and data caching.

6.1.2.7 Customer Information Control System (CICS Transaction Server)

CICS Transaction Server is a transaction manager that provides services for online transactions. CICS Transaction Server enhances the multiregion operation (MRO) links to provide more cross system communication for CICS. It supports the MVS workload manager component and VTAM generic resource. It also supports sysplex data sharing for IMS DB and DB2. CICS Transaction Server provides support for record-level sharing of data for VSAM.

6.1.2.8 CICSPlex System Manager/ESA (CICSPlex SM)

Provides a single-system image for a CICSPlex across a range of system management applications. These applications include dynamic workload balancing and separation in cooperation with the MVS workload manager, CICS master terminal operations, online access to CICS data and statistics, and the ability to detect exceptional events based on CICS state data for an operator or for automation purposes.

6.1.2.9 Operations Planning and Control (OPC/ESA)

OPC/ESA helps manage an installation's batch production workload. From one system plan, control, and monitor all workloads. OPC/ESA has been enhanced to present a single-system image in a sysplex environment. This enhancement will give a TSO user access to the OPC/ESA dialog even when the OPC/ESA Controller and the TSO user are active on different z/OS and OS/390 systems.

6.1.2.10 Workload Manager (WLM) – z/OS component

Manages workloads throughout a sysplex. WLM cooperates with transaction and resource managers that span systems. WLM uses customer-defined policies for performance objectives to help balance workloads.

6.1.2.11 System Automation for OS/390

System Automation for z/OS and OS/390 provides system automation for subsystem start and shutdown, automation for messages, timers, and system data set offload, and policy dialogs. System Automation for OS/390 also provides enterprise resource monitoring through a workstation graphical interface where the enterprise can include one or more sysplexes with coupling facilities.

6.1.2.12 Hardware Management Console

Hardware Management Console was enhanced to provide a single point of control for systems in a S/390 9672 Parallel Transaction Server and 9672 Parallel Enterprise Server. Through the use of icons and a mouse, operators can perform an operation for all systems or for a user-defined group of systems.

- *The IAO will ensure that the Hardware Management Console is restricted to authorized personnel.*

6.1.3 General Security Considerations

In a sysplex the security database could be shared across the sysplex. It uses the cross system coupling facility feature to handle cache and communication. It has been noted that reserve/release processing of the database could cause a fault if the system accessing the ACP database would fail. As a result, global enqueues will need to be set for the ACP database to be shared and coupling facility structures created. Sysplexes can be configured differently and the degree of security varies depending on the configuration of the software and hardware. The following areas should be considered:

1. Restrict the sysplex parmlib members as described in the Coupling Facility Section to authorized personnel.
2. Facility classes will need to be established for cross system coupling (ARM, CFRM, LOGR and SFM).
3. The UNIX couple data set `SYS1.OMVS.CDS01`, you do not need to perform any additional steps.
4. Policy structures updates will be restricted to authorized personnel.
5. The XCF couple data set format utility will need to be restricted to authorized personnel.
6. The WLM ISPF interface will need to be restricted to authorized personnel.
7. Define MCS consoles so that at least one console attached to a system is able to issue commands to another system in the sysplex.
8. Control automatic direction of commands, passwords, and application updates through profiles in the RRSFDATA class.

Note: The rules and permissions have not changed when migrating from a non-sysplex environment to a sysplex environment.

6.1.4 Sysplex Resource Classes

The following table describes possible resource classes that may be used with sysplexes. Check the appropriate security administrator guide for format and any additional requirements.

Resource Class	**Areas of Control**
IBMOPC	Controls access to OPC/ESA subsystems.
CPSMOBJ	Used by CICSPlex System Manager which provides a central point of control when running multiple CICS systems to determine operational
CPSMXMP	Used by CICSPlex System Manager to identify exemptions from security
ECICSDCT	Resource group class for DCICSDCT class, which is CICS destination control table.
GCICSTRN	Resource group class for TCICSTRN class.
GCPSMOBJ	Resource grouping class for CPSMOBJ.
HCICSFCT	Resource group class for FCICSFCT class, which is the CICS file control table.
KCICSJCT	Resource group class for JCICSJCT class, which is the journal control table.
NCICSPPT	Resource group class for MCICSPPT class which is the CICS processing program table.
QCICSPSB	Resource group class for PCICSPSB class, which is the program specification blocks or PSBs.

Resource Class	Areas of Control
UCICSTST	Resource group class for SCICSTST class which is the temporary storage table.
VCICSCMD	Resource group class for the CCICSCMD class which are the transactions.

Note: *The above resource classes might not be used depending on the resource.*

- *The IAO will ensure the above resource classes are used in sysplex security administration.*

6.4 ACF2

When coding rules for ACF2 check with the OS/390 STIG for formats by product. Additional information can be found in other sections of the LPAR STIG and the ACF2 Security Administrators Guide.

6.5 RACF

When coding rules for RACF check with the OS/390 STIG for formats by product. Additional information can be found in other sections of the LPAR STIG and the RACF Security Administrators Guide.

6.6 TOP SECRET

When coding rules for TSS checks with the OS/390 STIG for formats by product. Additional information can be found in other sections of the LPAR STIG and the TSS Security Administrators Guide.

7. COUPLING FACILITY

Vendor: IBM

7.1 General Considerations

In order to satisfy the need for multi-access to data on certain ES/9000 and S/390 processors, IBM developed a facility known as a coupling facility. A coupling facility is a shareable storage medium, but not what is usually considered a shared storage device. It is licensed internal code (LIC) running in a special type of PR/SM logical partition. A coupling facility provides high-speed caching, list processing, and locking functions in a systems complex (sysplex). Because of this, a coupling facility can be shared only by the systems in one systems complex (sysplex).

Hardware Configuration Definition (HCD) is used to define the components of a coupling facility I/O configuration. HCD provides the interface necessary to create the definitions and supplies the required channel control unit and I/O device definitions for the coupling facility channels. In addition, HCD is used to specify whether an LPAR is a coupling facility, operating system, or both on certain processors. Once the configuration has been created and activated in the IODF, PR/SM panels are used to define the coupling facility LPAR to the sysplex.

Coupling facility channels link a processor to a coupling facility. These coupling facility channels referred to as sender channels (CFS) and receiver channels (CFR) connect the coupling facility to the processor that is running MVS. These channels must be dedicated.

7.2 Types of Coupling Facility Structures

MVS recognizes three structure types—cache, list, and lock—and provides unique programming services for each of the structure types to allow the manipulation of data within the structure. To use these services, a system component, subsystem, or application **connects** to the structure, specifying a structure name and the type of structure it is. Following are descriptions of the three:

- **Cache structures** allow high-performance sharing of frequently referenced data.

- **List structures** enable users to share information organized as entries on a set of lists or queues.

- **Lock structures** allow users to create a customized set of locks and locking protocols for serializing user-defined resources, including list or cache structure data.

7.3 Couple Data Sets

A sysplex uses couple data sets to store information about its systems, the XCF groups and members running in the sysplex, and general status information. Couple data sets also contain policy information. A policy is a set of rules and actions that systems in a sysplex are to follow when using certain MVS services. A policy allows MVS to manage specific resources in compliance with your system and resource requirements, but with little operator intervention. A policy can be set up to govern all systems in the sysplex or only selected systems. As a result, additional couple data sets may be needed by the sysplex. The following couple data sets may be used:

- The **coupling facility resource management (CFRM) couple data set** holds the CFRM policy, which describes how MVS is to manage coupling facility resources.

- The **sysplex failure management (SFM) couple data set** holds the SFM policy, which defines how system failures, signaling connectivity failures, and PR/SM reconfiguration actions are to be managed.

- The **workload management (WLM) couple data set** holds the WLM policy, which defines service goals for workloads.

- The **automatic restart management (ARM) couple data set** holds the policy that defines how MVS is to manage restarts for specific batch jobs and started tasks that are registered as elements of automatic restart management.

- The **system logger (LOGR) couple data set** holds the policy that allows you to define log stream or structure definitions.

In order to avoid a single point of failure in the sysplex, IBM recommends that for all couple data sets, an alternate couple data set on a different device, control unit, and channel be created from the primary couple data set. An alternate couple data set provides additional advantages to the sysplex. By entering the OS/390 command **SETXCF COUPLE, PSWITCH,** the alternate couple data set can be dynamically changed to become the primary couple data set. Thus, in a non-disruptive way, the primary couple data set can be reformatted, moved to a different device, or defined to XCF. Because information about the sysplex and the services that use couple data sets is maintained in both the primary and alternate couple data sets concurrently, it is recommended that they reside on different DASD volumes. Also, ensure that the files are protected and appropriate workloads controlled, in accordance with site requirements. If the master catalog is not shared by all systems, ensure that the couple data set is in the master catalog of each system. The couple data sets must not be cataloged in a user catalog.

- *The coupling data sets will be restricted to authorized personnel. The log option will be turned on for all updates and accesses.*
- *The IAO will ensure that the **ARM, WLM, SFM, LOGR** coupling data sets are restricted to authorized personnel. The log option will be turned on for all updates and accesses.*

- *The IAO will ensure that the following **WLM TSO** files are protected from unauthorized update and use:*

SYS1.SBLSCLI0	-	*REXX code*
SYS1.SBLSKEL0	-	*WLM skeletons*
SYS1.SBLSPNL0	-	*WLM panels*
SYS1.SBLSTBL0	-	*WLM key lists and commands*
SYS1.SBLSMSG0	-	*WLM messages*

- *The **SETXCF COUPLE** commands will be restricted to authorized personnel. The log option will be turned on for all usage.*

IBM provides a couple data set format utility called IXCL1DSU to format the couple data sets. The format utility cannot use an existing couple data set. The couple data set must be created when the utility is run. The WLM couple data set can also be formatted interactively using the WLM administrative application. Because of the information contained in the couple data sets and their use, the IXCL1DSU utility and the WLM administrative application should be restricted to Systems Programmers and authorized personnel.

- *The IAO will ensure that the **IXCL1DSU** utility will be restricted to authorized personnel. The **log** option will be turned on for all accesses.*
- *The IAO will ensure that the **IXCMIAPU** utility will be restricted to authorized personnel. The **log** option will be turned on for all accesses.*

The couple data sets must be protected from being migrated or deleted by DFHSM. To prevent accidental expiration or migration of the volume by DFHSM, define the following management class attributes through the ISMF panels:

EXPIRE AFTER NON-USAGE=NOLIMIT
EXPIRE AFTER DATE/DAYS=NOLIMIT
COMMAND or AUTO MIGRATE=NONE

7.4 Authorizing Coupling Facility Requests

The Security Administrator must protect the integrity of the data within the structure before coupling facility requests such as IXLCONN, IXLREBLD, and IXLFORCE are issued. If a security server is installed, the administrator can define profiles that control the use of the structure in the coupling facility. This can be done through the external security manager.

The following steps describe how the Security Administrator defines profiles to control the use of structures:

(1) Define resource profile *profile-name.structure-name* using the ACP’s class restrictions.

(2) Specify the users who have access to the structure using the external security products command.

(3) Ensure that the ACP's class restrictions are active, and generic profile checking is active. If in-storage profiles are maintained, refresh them.

7.5 SYS1.PARMLIB Parameters and Members

Many of the values that represent the fundamental decisions made about the systems in the sysplex are in SYS1.PARMLIB. The list of parmlib members is needed to run a sysplex and the list provides a description of each parmlib member. All of the members must be named in accordance with DISA standards, DISA Computing Service's Naming Convention Standards, and protected from modifications by unauthorized personnel.

(1) IEASYSxx is the system parameter list, which holds parameter values that control the initialization of MVS. Some parameters identify other members of SYS1.PARMLIB that are to be used. (For example, the GRSCNF system parameter identifies the GRSCNFxx member.)

(2) COUPLExx contains parameter values that reflect sysplex-related information.

(3) GRSCNFxx describes the global resource serialization complex for the system.

(4) GRSRNLxx specifies the resource name lists to be used to control the serialization of resources in the complex.

(5) CLOCKxx indicates how the time of day is to be set on the system.

(6) IEASYMxx provides a single place to define system parameters and system symbols for all systems in a sysplex.

(7) LOADxx optionally specifies the name of the sysplex in which a system participates, which is also the substitution text for the &SYSPLEX system symbolic parameter.

(8) Multiple IEASYMxx parmlib members can be used to specify the system symbols and system parameters to be used.

(9) XCFPOLxx specifications are used only if a sysplex failure management policy is not active in the sysplex. Functions provided through XCFPOLxx can provide high availability for multisystem applications on an MVS system on PR/SM. If SFM is active in the sysplex, then the SFM policy specifications can define the same PR/SM reconfiguration actions that can be defined through XCFPOLxx.

(10) The CTIGXCFxx member is used to control the trace options of the Cross System Coupling Facility.

To prevent the number of parmlib definitions from increasing with each system that is added to a sysplex environment, share parmlib members across systems. If systems require unique values in those parmlib members, code them so that the different systems can supply unique values in shared parmlib definitions.

System symbolic parameters are the elements that allow systems to specify unique values in shared parmlib members. When specified in a parmlib definition that two or more system images are to share, system symbolic parameters resolve to unique values on each system.

- *The following members will be named in accordance with DISA standards as specified in DISA Computing Service's Naming Convention Standards:*

IEASYSxx
GRSCNFxx
CLOCKxx
LOADxx
CTIGXCFxx
COUPLExx
GRSRNLxx
IEASYMxx
XCFPOLxx

Note: *Where **xx** will be either **00** or **BK.** Alternate names will be justified and documented.*

7.6 Cross-System Coupling Facility (XCF)

7.6.1 General Considerations

The cross-system coupling facility (XCF) component enables authorized programs in a sysplex to communicate with programs on the same MVS system or other MVS systems. XCF services allow multiple instances of an application or subsystem, running on different systems in a sysplex, to share status information and communicate with each other. In addition, XCF provides the following:

- A capability to define a collection of unique parts of a program, and a way for each part to identify the other parts so they can work together.

- A method for parts of programs to send messages to, or receive messages from, other parts of programs on the same MVS system or on a different system, without regard for the I/O considerations involved. Messages can be sent without knowing specifically where the receiving part resides.

- A method for monitoring the program parts that a programmer defines to XCF. XCF maintains information about the defined program parts. These program parts can be on the same MVS system or other MVS systems.

- A way to design programs for high availability, such that primary parts are on one system and backup parts are on another system. Thus, when the primary system fails, XCF notifies the backup parts on the other system and the backup parts can be designed to take over the functions of the primary parts. The primary and backup parts can also be running in different address spaces on the same system. In this case, the parts running in the backup address space can be designed to take over when the primary address space fails.

- A way for batch jobs and started tasks to be restarted automatically. The XCF recovery function (referred to as automatic restart management), enables an application to be restarted automatically when it, or the system it is running on, fails.

7.6.2 XCF Communication Services

The communication services that XCF provides fall into three broad categories:

- **Group Services (Group and Member Relationships)**

  A **member** is a specific function (one or more routines) of a multisystem application that is defined to XCF and assigned to a group by the multisystem application. Through XCF group services, a member can identify an installation-written group user routine. XCF uses this routine to notify the member about changes that occur to members of the group, or systems in the sysplex. With a group user routine, members can have the most current information about the other members in their group without having to query communications services.

- **Signaling Services (Sending and Receiving Messages)**

  XCF signaling services are the primary means of communication between members of an XCF group. XCF uses assembled macros for sending and receiving messages.

- **Status Monitoring Services**

  XCF status monitoring services provide a way for members to actively participate in determining their own operational status, and to notify other members of their group when that operational status changes. XCF uses assembled macros to accomplish this.

Each of the macros as defined in the vendor documentation should be restricted to authorized Systems Programmers and loaded in restricted libraries.

7.6.3 XCF-Local Mode

In certain recovery scenarios, it might be necessary to have a system that can be initialized in XCF-local (standalone system) mode. A separate set of parmlib members could be used to IPL the systems in XCF-local mode. In that case an alternate LOADxx parameter may be placed in SYS1.PARMLIB that points to an IEASYSxx parmlib member that will be used to initialize a system in XCF-local mode. The IEASYSxx parmlib member and the LOADxx member in SYS1.PARMLIB should be named in accordance with DISA standards and protected from unauthorized access and modifications.

7.6.4 Security Considerations

The XCF address space (XCFAS) must be protected in accordance with DISA requirements. XCF does not need to be explicitly authorized to access couple data sets. The XCF started procedure must have an associated userid defined in the appropriate external security product's started procedures table. The started procedure name is XCFAS. The associated userid must have universal access to all sysplex resources.

A **group** is the set of related members defined to XCF by a multisystem application in which members of the group can communicate (send and receive data) between MVS systems with other members of the same group. A group can span one or more of the systems in a sysplex and represents a complete logical entity to XCF. Ensure that authorized systems personnel perform all group creation and maintenance.

A **multisystem application** is defined as a program that has various functions distributed across MVS systems in a multisystem environment. Ensure that all multisystem application programs are controlled in protected libraries.

A **member** is a specific function (one or more routines) of a multisystem application that is defined to XCF and assigned to a group by the multisystem application. A member resides on one system in the sysplex and can use XCF services to communicate (send and receive data) with other members of the same group. However, a member is not a particular task and is not a particular routine. The member concept applies to all authorized routines running in the address space in which the member was defined. The entire address space has the ability to act as that member. All tasks and SRBs in that address space can request services on behalf of the member. Members of XCF groups are unique within the sysplex. All member creation and maintenance must be restricted to authorized systems personnel and must be restricted to appropriate access.

This page is intentionally left blank.

8. INTEGRATED CRYPTOGRAPHIC SERVICES FACILITY (ICSF)

8.1 General Considerations

ICSF is an IBM software product that provides applications with the ability to perform cryptography. In the z/OS environment, ICSF runs as a started task, CSF. ICSF cryptographic services/routines work in conjunction with z/OS cryptographic coprocessors to perform the following types of functions:

- Cryptographic key generation and management
- Enciphering and deciphering of data using encrypted keys
- Transformation of CDMF data keys to shortened DES keys
- Re-enciphering of text data from encryption under one key to encryption under another key
- Encoding and decoding of data with clear keys
- Generation of random numbers
- Data integrity and authentication
- Generation, verification, and translating of personal identification numbers (PINs)

ICSF uses either the U.S. National Institute of Science and Technology Data Encryption Standard (DES) algorithm, or the Commercial Data Masking Facility (CDMF), a scrambling technique, to perform encryption/decryption. In addition, ICSF supports several types of Public Key Algorithms (PKA) that can be used to: exchange DES or CDMF secret keys securely, compute digital signatures, and authenticate messages and users. The ICSF callable services available to applications depend on the server configuration. They can be either DES with PKA and Triple DES with PKA.

- *The IAO will ensure that a started task class of **CSF** has been established and access restricted to authorized personnel and applications.*

8.1.1 Cryptographic Coprocessor

A Cryptographic Coprocessor is a hardware feature of a z/OS system. It can have up to two cryptographic coprocessor chips (crypto CPs), which serve as extensions of the central processor. Each crypto CP contains both DES and PKA cryptographic processors. The Cryptographic Coprocessor stores the cryptographic master keys internally in C-SRAM. The internal secure registers are not accessible through either Licensed Internal Code or scanning of the hardware.

Cryptographic Coprocessors are protected by tamper-detection circuitry that is designed to react to attacks by clearing all secure keys. The Cryptographic Coprocessor has two crypto CPs each of which is attached to a central processor complex. A processor complex can be configured to run in either single-image mode or logical partition mode. In single-image mode, the same master keys must be installed on both crypto CPs. If a second crypto CP is brought online, ICSF verifies that the master keys are the same. If the DES master keys are different, ICSF will not use the second Coprocessor. The PKA master keys must also be the same on both Coprocessors in order to enable the PKA services.

The cryptographic processors support multiple sets of master key registers, which the specific domain values identify. The Cryptographic Coprocessor has a master key register for the DES master key, the auxiliary DES master key, the signature master key and the key management master key. The auxiliary DES master key register may contain either the new or old DES master key. On the PCI Cryptographic Coprocessor, each domain has a master key register for the current, new, and old symmetric-keys master key (SYM-MK) and asymmetric-keys master key (ASYM-MK).

8.1.1.1 Allocating Cryptographic Resources to a Logical Partition

Logical Partitions LPs are able to utilize cryptographic functions through the use of the Hardware Management Console and Processor Resource/Systems Manager (PR/SM). Each PR/SM partition is able to use its own DES and PKA master keys on the Cryptographic Coprocessor and symmetric-keys master key (SYM-MK) and asymmetric-keys master key (ASYM-MK) on the PCI Cryptographic Coprocessor. This allows an installation to have multiple independent cryptographic systems running on the same processor with the same degree of isolation and protection as if they were running on physically separate processors.

To assign a control domain index, a usage domain index and to initially enable cryptographic coprocessor functions, use the Crypto page of the Customize Activation Profiles task. The following options can be enabled using the Crypto page for the LP:

- Public key algorithm (PKA) function
- Cryptographic functions
  – Special secure mode
  – Public key secure cable (PKSC) and Integrated Cryptographic Service Facility (ICSF)
- Modify authority (only enabled in one LPAR partition at a time)
- Query signature controls
- Query transport controls

- *The IAO will ensure that the Hardware Management Console will be restricted to authorized personnel.*
- *The IAO will ensure that the Crypto page of the Customize Activation Profile is restricted to authorized personnel.*

8.1.2 Keys

A key can be any combination of hexadecimal characters. They can be a string on characters, numbers or other keys. Keys can be either clear (readable) or encrypted. Because cryptographic algorithms are all key-controlled algorithms, the security of the cryptographic key is critical. With the exception of master keys, which are physically secured, all keys are enciphered to provide security. A key can be protected under a master key, a transport key, or a PKA key.

ICSF controls the use of keys by separating them into types that can be used to perform specific functions. To create an encrypted key, either a master key or a transport key is used to encrypt the base value of the key. ICSF encrypts data based on the type of key encountered. The following is a list of the types of DES keys supported by ICSF:

1. **DES Master Keys** used to protect DES and CDMF keys.
2. **Symmetric-Keys Master Key (SYM-MK)** is used only to encrypt other DES keys on the PCI Cryptographic Coprocessor.
3. **PKA Master Keys** are used only to encipher and decipher PKA keys. There are two PKA master keys on the Cryptographic Coprocessor. One PKA master key, the signature master key (SMK), protects private keys that are intended for creating digital signatures. The other PKA master key, the key management master key (KMMK), protects private keys that are used in DES key distribution.
4. **PKA Keys** are public keys which use either Rivest-Shamir-Adleman (RSA) or Digital Signature Standard (DSS).
5. **Asymmetric-Keys Master Key (ASYM_MK)** protects PKA private keys on the PCI Cryptographic Coprocessor.
6. **Transport Keys,** also known as key-encrypting keys, are used to protect keys when you distribute them from one system to another.
7. **Data-Encrypting Keys** are used to encipher and decipher data.
8. **Data-Translation Keys** are used for the ciphertext translate callable service as either the input or the output data-translation key.
9. **MAC Keys** are used for the callable services that generate and verify MACs.
10. **PIN Keys** are used for verifying the use identity across financial industry networks.
11. **Cryptographic Variable Encrypting Keys** are used to encrypt special control values in CCA DES key management.

The master key protects keys on the system. Keys sent to another system are protected using a transport key. RSA public keys protect DES data-encrypting keys that are transported between systems. Each key type is encrypted with a unique variation of the master key. ICSF creates a master key variant by manipulating the control vector on the key. Keys are considered active on a system only when they are encrypted under a master key variant. The ICSF administrator initializes and changes master keys using the ICSF panels under TSO. Master keys always remain in a secure area in the cryptographic hardware.

8.1.3 ICSF Data Sets

Multiple data sets are needed to support ICSF. Some are used for keys storage, ICSF programs and ISPF panels. The following subsections describe the data sets used by ICSF and security considerations.

8.1.3.1 Cryptographic Key Data Set (CKDS)

The Cryptographic Key Data Set CDKS is a key-sequenced VSAM data set used to store keys enciphered using the DES master key. The master key verification pattern is stored in the CKDS header record. A record in the CKDS is called a key entry and has a label associated with it. When an ICSF callable service needs to access a key on the CKDS data set, the key label is specified.

- *The IAO will ensure that the **SYS3.CSF.CKDS** data will be restricted to authorized personnel and applications through data set profiles of the ACP.*
- *The IAO will ensure that the **ERASE** and **WRITECHECK** parameters are used when creating the CKDS file.*
- *The IAO will ensure that all **UPDATE** and **ALLOCATE** is logged for the CKDS file.*

8.1.3.2 Public Key Data Set (PKDS)

The Public Key Data Set PKDS is a key-sequenced VSAM data set used to store Public Keys, and Public Key tokens. The PCI Cryptographic Coprocessor requires the PKDS. ICSF requires the PKDS to be available at start up.

- *The IAO will ensure that the **SYS3.CSF.PKDS** data will be restricted to authorized personnel and applications through data set profiles of the ACP.*
- *The IAO will ensure that the **ERASE** and **WRITECHECK** parameters are used when creating the PKDS file.*
- *The IAO will ensure that all **UPDATE** and **ALLOCATE** is logged for the PKDS file.*

8.1.3.3 Installation Options Data Set

The installation options data set contains the default options used by ICSF at startup. Because the installation options data set is a sequential file, it can reside as a member in SYS1.PARMLIB. The name of the member is CSFPRM00.

- *The IAO will ensure that the **CSFPRM00** resides in SYS1.PARMLIB and is restricted from unauthorized updates.*
- *The IAO will ensure that the following parameters are set in the options data set member:*

```
CKDSN  (SYS3.CSF.CKDSN)
PKDSN  (SYS3.CSF.PKDSN)
SSM      (YES)
COMPENC  (DES)
CHECKAUTH  (YES)
KEYAUTH  (YES)
```

8.1.4 ICSF Administration

ICSF administration involves many different types of activities. They range from creating and maintaining keys, creating and maintaining ICSF data sets, setting cryptographic coprocessor defaults and managing callable services. ICSF administration can be done either through ICSF ISPF panels or through the use of utility programs. The following subsections describe both the utilities that can be used to accomplish these functions and the ICSF ISPF panels that can also be used.

8.1.4.1 ICSF Utility Programs

ICSF provides three utility programs to perform system administration. They are the CSFKGUP utility, the CSFEUTIL utility and the CSFPUTIL utility. It should be noted that these programs can be linked to by other programs and will need to be restricted.

8.1.4.1.1 The Key Generator Utility Program (KGUP)

The key generator utility program **CSFKGUP** is used to generate and maintains keys in the cryptographic key data set (CKDS). Maintenance is performed by deleting or renaming entries in the CKDS. In order to run KGUP the following must occur: ICSF must be active, it must contain a master key, and the CKDS must be initialized.

KGUP uses control statements to specify the functions for KGUP to perform. The control statements specify the task you want KGUP to perform, and information about the CKDS entry. When KGUP processes the control statement, the program generates a key value and encrypts the value under a master key variant for an importer key-encrypting key. Control statements used by KGUP are stored in a data set. To prevent unauthorized access to the KGUP, the program will be placed in an APF-authorized library that is protected by the ACP.

- *The IAO will ensure that the **CSFKGUP** utility is located in an APF authorized library.*
- *The IAO will ensure that the **CSFKGUP** utility is restricted to authorized personnel.*
- *The IAO will ensure that a **log** is maintained of all maintenance performed on the CKDS and PFDS data sets.*

8.1.4.1.2 The CSFEUTIL Utility Program

ICSF provides the utility program, **CSFEUTIL** to perform functions that can also be performed using the administrator’s panels. The utility can be used with the cryptographic coprocessor feature and the PCI cryptographic coprocessor feature. This utility can be run to perform the following tasks:

- Re-encipher a disk copy of a CKDS
- Change the master key
- Refresh the in-storage CKDS
- Initialize a CKDS and load DES and PKA master keys using a pass phrase

The utility can be run as a batch job or invoked from another program. A PARM value is passed to the program to tell the program what function is to be performed.

- *The IAO will ensure that the* **CSFEUTIL** *utility is restricted to authorized personnel.*
- *The IAO will ensure that a **log** is maintained of all maintenance performed on the CKDS and PFDS data sets.*

8.1.4.1.3 The CSFPUTIL Utility Program

ICSF provides the utility program, **CSFPUTIL** to perform functions that can also be performed using the administrator's panels. The utility can be used with the cryptographic coprocessor feature and the PCI cryptographic coprocessor feature. This utility can be run to perform the following tasks:

- Re-encipher a PKDS
- Activate the re-enciphered PKDS
- Refresh the PKDS cache

The utility program can be run as a batch job or from another program. The function performed is specified through a PARM value supplied to the program.

- *The IAO will ensure that the* **CSFPUTIL** *utility is restricted to authorized personnel.*
- *The IAO will ensure that a* ***log*** *is maintained of all maintenance performed on the CKDS and PFDS data sets.*

8.1.5 ICSF Panels

ICSF can be administered using ISPF ICSF panels. The types of administration can vary from key management to ICSF configuration. In addition, ICSF panels can be used to control the cryptographic coprocessors. As a result, ICSF panel security under ISPF is required.

- *The IAO will ensure that the ICSF ISPF data sets are protected from unauthorized access and updates. The data sets are:*

  SYS3.CSF.SCSFCLI0
  SYS3.CSF.SCSFPNL0
  SYS3.CSF.SCSFMSG0
  SYS3.CSF.SCSFSKL0
  SYS3.CSF.SCSFTLIB

- *The IAO will ensure that the ICSF option in TSO is restricted to authorized personnel.*
- *The IAO will ensure that all* ***UPDATE*** *and* ***ALLOCATE*** *is logged for the ICSF Panels.*

8.1.6 ICSF Exits

ICSF can be tailored using ICSF EXITs. ICSF exits can be invoked at various stages of ICSF processing. ICSF exits can be invoked when an operator command starts, stops, or changes ICSF, when the CKDS data set is accessed and when the in-storage CKDS is accessed by an application. The following tables describe, categorize and list the ICSF exits. Further information about each of the exits can be found in the *IBM Systems Programmer's Guide for ICSF*.

General ICSF Exits and Exit Identifiers (8.1.6 a)

General ICSF Exit	Exit Identifier
Conversion Exit	CSFCONVX
Cryptographic Key Data Set Retrieval Exit	CSFCKDS
Key Generator Utility Program Exit	CSFKGUP
Mainline Exits	CSFEXIT2, CSFEXIT3, CSFEXIT4, CSFEXIT5
Security Initialization Exit Point	CSFESECI
Security Key Exit Point	CSFESECK
Security Service Exit Point	CSFESECS
Security Termination Exit Point	CSFESECT
Single-record Read-write Exit Point	CSFSRRW

Callable Service and its Exit Identifier (8.1.6 b)

Service	Exit Identifier
ANSI X9.17 EDC generate	CSFAEGN
ANSI X9.17 Key Export	CSFAKEX
ANSI X9.17 Key Import	CSFAKIM
ANSI X9.17 Key Translate	CSFAKTR
ANSI X9.17 Transport Key Partial Notarize	CSFATKN
Clear PIN Encrypt	CSFCPE
Clear PIN Generate Alternate	CSFCPA
Clear Key Import	CSFCKI
Cipher/Decipher	CSFEDC
Cipher Text Translate	CSFCTT
Cipher Text Translate (with ALET)	CSFCTT1
Control Vector Translate	CSFCVT
Cryptographic Variable Encipher	CSFCVE
Data Key Import	CSFDKM
Decode	CSFDCO
Decipher	CSFDEC
Decipher (with ALET)	CSFDEC1
Data Key Export	CSFDKX
Digital Signature Generate	CSFDSG
Digital Signature Verify	CSFDSV
Diversified Key Generate	CSFDKG
Encode	CSFECO
Encipher under Master Key	CSFEMK
Encipher	CSFENC
Encipher (with ALET)	CSFENC1
Encrypted PIN Generate	CSFEPG
Key Export	CSFKEX
Key Generate	CSFKGN

Service	Exit Identifier
Key Import	CSFKIM
Key Part Import	CSFKPI
Key Record Create	CSFKRC
Key Record Delete	CSFKRD
Key Record Read	CSFKRR
Key Record Write	CSFKRW
Key Test	CSFKYT
Key Test Extended	CSFKYTX
Key Translate	CSFKTR
MAC Generate	CSFMGN
MAC Generate (with ALET)	CSFMGN1
MAC Verify	CSFMVR
MAC Verify (with ALET)	CSFMVR1
MDC Generate	CSFMDG
MDC Generate (with ALET)	CSFMDG1
Multiple Clear Key Import	CSFCKM
Multiple Secure Key Import	CSFSCKM
One-Way Hash Generate	CSFOWH
One-Way Hash Generate (with ALET)	CSFOWH1
PCI Interface	CSFPCI
PIN Generate	CSFPGN
PIN Translate	CSFPTR
PIN Verify	CSFPVR
PKA Decrypt	CSFPKD
PKA Encrypt	CSFPKE
PKA Key Generate	CSFPKG
PKA Key Import	CSFPKI
PKA Key Token Change	CSFPKTC
PKDS Record Create	CSFPKRC
PKDS Record Delete	CSFPKRD
PKDS Record Read	CSFPKRR
PKDS Record Write	CSFPKRW
Prohibit Export	CSFPEX
Prohibit Export Extended	CSFPEXX
Random Number Generate	CSFRNG
Retained Key Delete	CSFRKD
Retained Key List	CSFRKL
Secure Key Import	CSFSKI
Secure Messaging for Keys	CSFSKY
Secure Messaging for PINs	CSFSPN
SET Block Compose	CSFSBC
SET Block Decompose	CSFSBD
Symmetric Key Generate	CSFSYG
Symmetric Key Import	CSFSYI

Service	Exit Identifier
Symmetric Key Export	CSFSYX
Transform CDMF Key	CSFTCK
User Derived Key	CSFUDK
VISA CVV Service Generate	CSFCSG
VISA CVV Service Verify	CSFCSV

Compatibility and its Exit Identifier (8.1.6 c)

Compatibility	Exit Identifier
Encipher under Master Key	CSFEMK
CUSP/PCF GENKEY Service	CSFGKC
CUSP/PCF RETKEY Service	CSFRTC
Cipher/Decipher	CSFEDC

- *The IAO will ensure that the above ICSF exits are restricted to authorized personnel.*
- *The IAO will ensure that the uses of the above ICSF exits are restricted to authorized personnel and applications.*
- *The IAO will ensure that FSO reviews any GOTs exit before implementation into production.*

8.1.7 ICSF Event Recording

ICSF uses System Management Facilities SMF record type 82 records to record ICSF events in the SMF data set. The SMF recording and messages help detect potential problems and track events. The ICSF Systems Programmers Guide provides the details of the types of information recorded.

- *The IAO will ensure that ICSF events are recorded using the SMF Type 82 records and stored in the SMF data sets. Access to the SMF data sets will be restricted to authorized personnel.*

8.2 General Security Considerations

Securing ICSF is accomplished by restricting access to ICSF resources and services. This is done through the system ACP. The following areas must be addressed when securing ICSF:

1. Access to Disk Copies of the CKDS.
2. Access to the PKDS.
3. Access to the Key Generator Utility Program (KGUP).
4. Access to the CSFEUTIL and CSFPUTIL utilities.
5. Access to Services and Keys.
6. Access to the CSF started task.
7. Access to the ICSF ISPF panels.

Note: *The **in-storage** copy of the **CKDS** can be accessed only through ICSF functions such as Callable services, KGUP, or the ICSF panels.*

It is recommended by IBM that changes of Cryptographic Keys and the DES Master Key be scheduled on a regular basis.

- *The IAO will ensure that the access to the in-storage copy of the CKDS is restricted to authorized personnel and applications.*
- *The IAO will ensure that CSFSERV and CSFKEYS classes have been created to perform access checking and auditing of services and keys.*
- *The IAO will ensure that the access to the CSF started task is restricted to authorized personnel and applications.*
- *The IAO will ensure that the CSF startup procedure is located in SYS1.PROCLIB.*
- *The IAO will ensure that the ICSF ISPF panels are restricted to authorized personnel.*
- *The IAO will ensure that the* ***SYS1.CSF.SCSFMOD0*** *data set is link listed.*
- *The IAO will ensure that the member* ***IKJTSO00*** *contains* ***CSFDAUTH*** *specified in the* ***AUTHPGM*** *and* ***AUTHTSF*** *sections.*
- *The IAO will ensure that ICSF services are restricted to authorized personnel and applications.*

8.3 CA-ACF2 Implementation

The following guidelines are provided to assist in the setup of ICSF under CA-ACF2. They were developed in conjunction with *section 8.2*.

(1) Create a valid STC userid and define the appropriate access rules for the ICSF distribution and installation libraries.

(2) Create the logonid for the CSF STC:

```
INSERT CSF NAME(CSF, STC, SMRTCRD) STC NO-SMC
```

(3) Create/modify access rule sets:

```
$KEY(SYS1)
   CSF.- UID(CSF) R(A) W(A) E(A)                   ICSF Started Task
   CSF.SCSFMOD0 UID(CSF) R(A) E(A)                 ICSF Started Task
   CSF.- UID(user) R(A) W(L) A(L) E(A)             Systems and Security only
   CSF.SCSFMOD0 UID(user) R(A) W(L) A(L) E(A)      Systems
   CSF.SCSFMOD0 UID(user) R(A) E(A)                Security
   CSF.- UID(user) R(A)                        CA-EXAMINE Auditors CSF.-
   UID(*)                                          All others
*
$KEY(SYS3)
   CSF.- UID(CSF) R(A) W(A) E(A)                   ICSF Started Task
   CSF.- UID(user) R(A) W(L) A(L) E(A)             Systems and Security only
   CSF.- UID(user) R(A)                            CA-EXAMINE Auditors
   CSF.- UID(*)                                    All others
```

(5) Create CLASMAPs for CSFKEYS and CSFSERV.

```
SET CONTROL(GSO)
INSERT CLASMAP.CSFKEYS RESOURCE(CSFKEYS) RSRCTYPE(CSK)
      ENTITYLN(73)
INSERT CLASMAP.CSFSERV RESOURCE(CSFSERV) RSRCTYPE(CSF)
      ENTITYLN(8)
```

(6) Create/modify access rule sets for CSFSERV and CSFKEYS to allow access to authorized users and applications.

8.4 CA-TOP SECRET Implementation

The following guidelines are provided to assist in the setup of ICSF under CA-TOP SECRET. They were developed in conjunction with *section 8.2*.

(1) Create a valid STC userid and define the appropriate access rules for the CSF distribution and installation libraries.

(2) Create an ACID for the started task called **CSF** with **FACILITY** of **STC**. Include other data as pertinent to the site.

```
TSS CRE(CSF) DEPT(Dept) NAME('CSF, STC, SMRTCRD')
    FAC(STC) PASSWORD(password,0)
    SOURCE(INTRDR)
```

The following is a *sample* **CSF** ACID definition:

```
ACCESSORID  = CSF              NAME          = CSF, STC, SMRTCRD
TYPE        = USER             SIZE          = 512  BYTES
FACILITY    = STC
DEPT ACID   = STCDEPT          DEPARTMENT    = STC DEPT
DIV ACID    = TECHDIV          DIVISION      = TECH SUPPORT DIVISION
ZONE ACID   = SOFTZONE         ZONE          = SOFTWARE ZONE
CREATED     = 02/28/03         LAST MOD      = 03/01/03  09:42
LAST USED   = 03/01/03 10:36 CPU(WP27) FAC(STC     ) COUNT(00018)
```

(3) Define the ICSF started task to TSS Start Task Table:

```
TSS ADD(STC) ACID(CSF) PROCN(CSF)
```

(4) Grant permissions to the ICSF data sets to personnel as required:

Systems and Security:

```
TSS PERMIT(acid) DSN(SYS1.CSF.) ACCESS(ALL)
      ACTION(AUDIT)
```

```
TSS PERMIT(acid) DSN(SYS1.CSF.SCSFMOD0) ACCESS(READ)
TSS PERMIT(acid) DSN(SYS3.CSF.) ACCESS(ALL)
      ACTION(AUDIT)
```

Systems:

```
TSS PERMIT(acid) DSN(SYS1.CSF.SCSFMOD0) ACCESS(ALL)
      ACTION(AUDIT)
```

ICSF Started Task:

```
TSS PERMIT(CSF) DSN(SYS1.CSF.) ACCESS(UPDATE)
TSS PERMIT(CSF) DSN(SYS1.CSF.SCSFMOD0) ACCESS(READ)
TSS PERMIT(CSF) DSN(SYS3.CSF.) ACCESS(UPDATE)
```

CA-EXAMINE Auditors:

```
TSS PERMIT(acid) DSN(SYS1.CSF.) ACCESS(READ)
TSS PERMIT(acid) DSN(SYS3.CSF.) ACCESS(READ)
```

(5) Create/modify access rule sets for CSFSERV and CSFKEYS to allow access to authorized users and applications.

8.5 RACF Implementation

The following guidelines are provided to assist in the setup of ICSF under RACF. They were developed in conjunction with *section 8.2*.

(1) Create a STC userid for the **CSF** started task. The userid will be defined as a **PROTECTED** userid. For example:

```
AU CSF NAME('CSF, STC, SMRTCRD') NOPASSWORD
    OWNER(admin) DFLTGRP(STC) PROTECTED
```

(2) Ensure the CSF STC has a matching profile defined to the **STARTED** resource class. Issue the following command to define the profile:

```
RDEFINE STARTED CSF.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STC))
```

(3) Add the rule for CSF non-customized data sets:

```
AD 'SYS1.CSF.**' UACC(NONE) AUDIT(SUCCESS(UPDATE)
    FAILURE(READ))
AD 'SYS1.CSF.SCSFMOD0.**' UACC(NONE) AUDIT(SUCCESS(UPDATE)
    FAILURE(READ))
```

(4) Add the rule for CSF customized data sets:

AD 'SYS3.CSF.' UACC(NONE) AUDIT(SUCCESS(UPDATE)
FAILURE(READ))**

(5) Grant permissions to the CSF data sets to personnel as required:

Systems:

PE 'SYS1.CSF.' ID(*xxxxxx*) ACC(ALTER)**
PE 'SYS1.CSF.SCSFMOD0.' ID(*xxxxxx*) ACC(ALTER)**
PE 'SYS3.CSF.' ID(*xxxxxx*) ACC(ALTER)**

Security:

PE 'SYS1.CSF.' ID(*xxxxxx*) ACC(ALTER)**
PE 'SYS1.CSF.SCSFMOD0.' ID(*xxxxxx*) ACC(READ)**
PE 'SYS3.CSF.' ID(*xxxxxx*) ACC(ALTER)**

ICSF Started Task:

PE 'SYS1.CSF.' ID(CSF) ACC(UPDATE)**
PE 'SYS1.CSF.SCSFMOD0.' ID(CSF) ACC(READ)**
PE 'SYS3.CSF.' ID(CSF) ACC(READ)**

CA-EXAMINE Users/Auditors:

PE 'SYS1.CSF.' ID(*xxxxxx*) ACC(READ)**
PE 'SYS1.CSF.SCSFMOD0.' ID(*xxxxxx*) ACC(READ)**
PE 'SYS3.CSF.' ID(*xxxxxx*) ACC(READ)**

(6) Create/modify access rule sets for CSFSERV and CSFKEYS to allow access to authorized users and applications.

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense (DOD) Directive 8500.1, "Information Assurance (IA),” October 24, 2002.

Department of Defense (DOD) Directive 8500.1, "DOD Trusted Computer System Evaluation Criteria," October 24, 2002.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," July 1996.

Defense Information Systems Agency (DISA) Computing Services Naming Convention Standards, February 1996.

Defense Information Systems Agency (DISA) Computing Services Security Handbook, Version 3, 1 December 2000.

Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide, Version 4, Release 2, 15 October 2002.

Defense Information Systems Agency (DISA) UNIX Security Technical Implementation Guide, Version 3, Release 1.1, 5 January 2001.

Defense Information Systems Agency (DISA) OS/390 Security Technical Implementation Guide, Version 3, Release 2, 30 June 2002.

Defense Information Systems Agency (DISA) VM Security Technical Implementation Guide, Version 1, Release 3, 29 April 2002.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," October 9, 1991.

Army Regulation (AR) 380-19, "Information Systems Security," 1 August 1990.

Air Force Systems Security Instruction (AFSSI) 5100, "The Air Force Computer Security (COMPUSEC) Program," June 2, 1992.

Air Force Systems Security Memorandum (AFSSM) 5007, "A Methodology for Addressing DOD-Mandated "C2 by 92" for Operational Air Force Systems," March 25, 1991.

Secretary of the Navy Instruction (SECNAVINST) 5239.2, "Department of the Navy Automated Information Systems (AIS) Security Program," November 15, 1989.

Navy Staff Office Publication (NAVSO Pub) 5239-15, "Controlled Access Protection Guidebook," August 1992.

Public Law 100-235, 100th Congress, an Act cited as the "Computer Security Act of 1987," January 8, 1988.

Executive Office of the President, Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources," December 12, 1985.

International Business Machines Corporation Publications

- OS/390 MVS Initialization and Tuning Reference (SC28-1752)
- OS/390 MVS System Management Facilities (SMF) (GC28-1783)
- OS/390 MVS System Commands (GC28-1781)
- OS/390 SecureWay Communications Server IP Configuration (SC31-8513)
- OS/390 Security Server (RACF) Callable Services (GC28-1921)
- NetView Administration and Reference, Version 2
- NetView Installation and Operations Guide, Version 2
- OS/390 CDROM
- JES2 Implementation Guide

Computer Associates Corporation Publications

CA-EXAMINE Product Manuals
CA-ACF2 Product Manuals
CA-TOP SECRET Product Manuals

Other

TMON for MVS Product Manuals
TMON for CICS Product Manuals
FDR Product Manuals
OMEGAMON/OMEGAMON II Product Manuals

APPENDIX B. LIST OF ACRONYMS

ACP	Access Control Program. A program controlling resource access such as ACF2, RACF, or TOP SECRET.
AIS	Automated Information Systems (data processing systems).
CHPID	Channel Path Identifier. The identification number for a channel address.
CPU	Central Processing Unit.
DAC	Discretionary Access Control.
DASD	Direct Access Storage Device. The IBM name for disk storage.
DB	Database. A collection of data values stored in a file or group of files to simplify access and control.
DBMS	Database Management System. A type of software product designed to increase the availability of data, establish relationships between data elements, and ease the orderly processing of the data contained within the database.
DECC	Defense Enterprise Computing Center.
DECC-D	Defense Enterprise Computing Center-Detachment.
DOD-CERT	Department of Defense Computer Emergency Response Team (*formerly ASSIST*).
Domain	A processing environment consisting of main storage, channels, operator facilities, and logical and/or physical processors used to permit the operation of a SCP. A Logical Partition.
EDT	Eligible Device Table. The portion of the I/O *gen* containing the modules required for MVS to access the hardware devices. Refer to *SYS1.NUCLEUS*.
EMIF	ESCON Multiple Image Facility. This facility allows multiple logical partitions to share ESCON channels and optionally to share any of the control units and associated I/O devices configured to these shared ESCON channels. Refer to *ESCON*.
EOP	Executive Office of the President (part of the Office of Management and Budget).

ESCON	Enterprise Systems Connection. A set of products and services that provides a dynamically connected environment using optical cables as a transmission medium.
GNOSC	Global Network Operations and Security Center (formerly *GOSC*).
HCD	Hardware Configuration Definition. An interactive MVS component that performs both the functions of MVSCP and IOCDS. Refer to *IODF*.
HDS	Hitachi Data Systems.
HSA	Hardware Save Area.
IBM	International Business Machines.
IDMS	Integrated Database Management System.
I/O	Input/Output.
IOCDS	Input/Output Configuration Data Set.
IOCP	Input/Output Configuration Program. Used by MVS to perform the I/O configuration within MVS. Refer to *MVSCP*.
IODF	Input/Output Definition File. Used by HCD to store the I/O configuration information. Refer to *HCD*.
IPL	Initial Program Load. The process initiating an MVS operating system instance (domain).
ISPF	Interactive System Productivity Facility. A full-screen editing and data manipulation product that runs on top of IBM's Time Sharing Option (TSO). Refer to *TSO*.
IAM	Information Assurance Manager.
IAO	Information Assurance Office.
LP	Logical Processor (specific to the Amdahl Corporation). A logical processor is a software representation of the hardware components that comprise an LPAR.
LPAR	Logical Partition (specific to the IBM Corporation). A group of hardware components (usually a subset) that is defined to support the operation of a SCP (a domain).

LPDEF
Logical Partitioning Definition frame on an IBM hardware console to manipulate the different partitions.

LPRCTL
Logical Partitioning Control frame used on a Hitachi Data Systems processor.

MDF
Multiple Domain Feature. (Amdahl's implementation of the partitioning of the hardware on a single machine.

MLPF
Multiple Logical Processor Facility. Hitachi Data Systems' implementation of the partitioning of the hardware on a single machine.

MLS
Multi-level Security. The process of permitting several classifications of data in one domain (e.g., **Secret** and **Top Secret** data) and using the ACP to prevent unauthorized personnel from accessing data for which they are not cleared, or for which they do not have a need-to-know.

MVS
Multiple Virtual Storage.

MVSCP
MVS Configuration Program. The program that builds the MVS Input/Output image [part of MVS]). Refer to *IOCP*.

NIPRNet
Non-classified (but Sensitive) Internet Protocol Routing Network.

Operating System
A suite of programs/software that acts as the interface between the hardware and the application programs (the same as a system control program).

OPRCTL
Operator Control frame on an IBM processor to perform an IPL.

OS/390 Logical Partition STIG
OS/390 Logical Partition Security Technical Implementation Guide. The document providing the standards and implementation requirements necessary while running multiple logical partitions or domains in a single-processor environment.

POR
Power On Reset. Refer to *SYSIML*.

Processor
A central processing unit.

PR/SM
Processor Resource/Systems Manager. IBM's implementation of partitioning hardware on a single machine.

RNOSC
Regional Network Operations and Security Center (formerly *ROSC*).

SCP System Control Program. (Has the same meaning as an operating system. In the context of this document, it means a version of MVS, unless otherwise stated.)

SIPRNet Secret Internet Protocol Router Network.

SRR Security Readiness Review. The verification process for validating that the security requirements have been met.

SSM Site Security Manager.

SSO Systems Support Office.

STIG Security Technical Implementation Guide. A document describing the requirements and methodology for implementing security in the DISA environment.

SYS1.NUCLEUS Data set used by MVS that contains the load modules necessary to initialize the system. It also includes the EDT. Refer to *EDT*.

SYSIML System Initial Microcode Load. This performs the same function as a POR on an IBM processor. Refer to *Power On Reset.*

TSO Time Sharing Option. A line editor and data manipulation product enabling multiple users to log on and share the system in an interactive manner. An early IBM editor. Refer to *ISPF*.

UCB Unit Control Block. The information about an I/O device necessary for MVS to communicate with each device. A UCB exists for each I/O device in a configuration. Refer to *UIM*.

UIM Unit Information Module. A structure that defines the Unit Control Blocks for the I/O *gens*. Refer to *UCB.*

XCF Cross System Coupling Facility. A component that enables authorized programs in a sysplex to communicate with programs on other MVS systems.

APPENDIX C. AREA OF RESPONSIBILITY AND LPAR POLICIES

The following is a concise breakdown of area of responsibility followed by the policy that must be carried out and the individual who is ultimately responsible for the procedure.

Organizational Relationships

- *The IAO will maintain access based on approved personnel security investigations/security clearances, need-to-know, and written authorization.*
- *The IAO will maintain a log of all dial-out to vendors for maintenance.*

Security through the Access Control Product

- *IAOs will develop supplemental procedures, as required, in consonance with INFOCON guidance.*

Extensions

- *As part of the LPAR SRR review, the IAO will fill in and provide a copy of the Documentation Worksheet, Access Control Product (ACP) Worksheet, Central Processor Complex Domain/LPAR Names Table and Vendor Products List to the FSO SRR team. The sheets can be found in the LPAR checklist.*

Input/Output Configuration Program (IOCP)

- *The IAO will create and maintain ACP data set rules for the* ***IOCP*** *program. The rules will restrict access to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*

Hardware Configuration Definition (HCD) Program

- *The IAO will ensure that the IOCP utility (ies) is (are) defined using the* ***PROGRAM*** *resource class and restricted to authorized personnel. The IAO will also ensure that access to the program is logged.*
- *The IAO will create and maintain ACP data set rules for the* ***IODFxx.WORK*** *data set. The rules will restrict access to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*

- *The IAO will create and maintain ACP data set rules for the* ***IODFxx*** *data set. The rules will restrict access to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*
- *The IAO will create and maintain ACP rules that restrict read and update access of* ***CBD*** *prefixed resources to authorized personnel. The logging option will be turned on for all access.*
- *The IAO will create and maintain ACP rules restricting access to the* ***ACTLOG*** *log data sets to authorized personnel. The logging option will be turned on for UPDATE and/or ALTER access.*

- *The IAO will create and maintain ACP rules restricting access to authorized personnel for the following data sets:*

SYS1.SCBDHENU	**(FMID)**
SYS1.SCBDCLST	**(CLIST)**
SYS1.SCBDPENU	**(PANELS)**
SYS1.SCBDMENU	**(MESSAGES)**
SYS1.SCBDTENU	**(TABLES)**

- *The IAO will create and maintain ACP rules restricting access to the **ACTIVATE** command to authorized personnel. The logging option will be turned on for all accesses.*

HCD

- *The IAO will ensure that the LOADxx members are named in accordance with DISA standards and follow the guidelines specified in DISA Computing Service's Naming Convention Standards handbook.*

DISA Physical Requirements for the Test LPAR Environment

- *The IAO will ensure that that Hardware Management Console is located in a controlled area and access to the Hardware Management Console is restricted to authorized personnel.*
- *The IAO will ensure that micro-code updates to the Hardware Management Console are tracked.*

DISA Physical Requirements for the Production LPAR Environment

- *The IAO will ensure that that Hardware Management Console is located in a controlled area and access to the Hardware Management Console is restricted to authorized personnel.*
- *The IAO will ensure that micro-code updates to the Hardware Management Console are tracked.*

DISA Physical Requirements for the Classified LPAR Environment

- *The IAO will maintain written procedures for handling the introduction of classified information into the system.*
- *The IAO will ensure that automatic dial-out access to the Hardware Management Console is not activated for classified LPARs.*
- *The IAO will ensure that the automatic dial-in facility is restricted for classified LPARs.*

DISA Maintenance Requirements for the Classified LPAR Environment

- *The IAO will ensure that the automatic dial-in facility for classified LPARs is restricted.*

DISA Physical Requirements for the Restricted LPAR Environment

- *The IAO will maintain written procedures for handling the introduction of restricted information into the system.*
- *The IAO will ensure that automatic dial-out access to the Hardware Management Console is not activated for restricted LPARs.*
- *The IAO will ensure that the automatic dial-in facility is restricted for restricted LPARs.*

ESCON Manager Commands

- *The IAO will ensure that the ESCON Manager Commands are restricted to authorized personnel. The log option will be enabled for all accesses.*

Cross System Coupling (XCF)

- *The IAO will ensure that ACP rules exist restricting update access the XCF data sets.*
- *The IAO will ensure that the facility resource classes are created for XCF.*

Hardware Management Console

- *The IAO will ensure that the Hardware Management Console is restricted to authorized personnel.*

Sysplex Resource Classes

- *The IAO will ensure that the above resource classes are used in sysplex security administration.*

Couple Data Sets

- *The IAO will ensure that the **ARM** coupling data sets are restricted to authorized personnel. The log option will be turned on for all updates and accesses.*
- *The IAO will ensure that the **WLM** coupling data sets are restricted to authorized personnel. The log option will be turned on for all updates and accesses.*
- *The IAO will ensure that the **SFM** coupling data sets are restricted to authorized personnel. The log option will be turned on for all updates and accesses.*
- *The IAO will ensure that the **LOGR** coupling data sets are restricted to authorized personnel. The log option will be turned on for all updates and accesses.*
- *The IAO will ensure that the following **WLM** files are protected from unauthorized update and use:*

SYS1.SBLSCLI0	-	*REXX code*
SYS1.SBLSKEL0	-	*WLM skeletons*
SYS1.SBLSPNL0	-	*WLM panels*
SYS1.SBLSTBL0	-	*WLM key lists and commands*
SYS1.SBLSMSG0	-	*WLM messages*

- *The IAO will ensure that the **IXCL1DSU** utility will be restricted to authorized personnel. The **log** option will be turned on for all accesses.*
- *The IAO will ensure that the **IXCMIAPU** utility will be restricted to authorized personnel. The **log** option will be turned on for all accesses.*

General Considerations

- *The IAO will ensure that a started task class of **CSF** has been established and access restricted to authorized personnel and applications.*

Allocating Cryptographic Resources to a Logical Partition

- *The IAO will ensure that the Hardware Management Console will be restricted to authorized personnel.*
- *The IAO will ensure that the Crypto page of the Customize Activation Profile is restricted to authorized personnel.*

Cryptographic Key Data Set (CKDS)

- *The IAO will ensure that the **SYS3.CSF.CKDS** data will be restricted to authorized personnel and applications through data set profiles of the ACP.*
- *The IAO will ensure that the **ERASE** and **WRITECHECK** parameters are used when creating the CKDS file.*
- *The IAO will ensure that all **UPDATE** and **ALLOCATE** is logged for the CKDS file.*

Public Key Data Set (PKDS)

- *The IAO will ensure that the **SYS3.CSF.PKDS** data will be restricted to authorized personnel and applications through data set profiles of the ACP.*
- *The IAO will ensure that the **ERASE** and **WRITECHECK** parameters are used when creating the PKDS file.*
- *The IAO will ensure that all **UPDATE** and **ALLOCATE** is logged for the PKDS file.*

Installation Options Data Set

- *The IAO will ensure that the **CSFPRM00** resides in SYS1.PARMLIB and is restricted from unauthorized updates.*
- *The IAO will ensure that the following parameters are set in the options data set member:*

```
CKDSN  (SYS3.CSF.CKDSN)
PKDSN  (SYS3.CSF.PKDSN)
SSM       (YES)
COMPENC  (DES)
CHECKAUTH  (YES)
KEYAUTH  (YES)
```

The Key Generator Utility Program (KGUP)

- *The IAO will ensure that the **CSFKGUP** utility is located in an APF authorized library.*
- *The IAO will ensure that the **CSFKGUP** utility is restricted to authorized personnel.*
- *The IAO will ensure that a **log** is maintained of all maintenance performed on the CKDS and PFDS data sets.*

The CSFEUTIL Utility Program

- *The IAO will ensure that the* **CSFEUTIL** *utility is restricted to authorized personnel.*
- *The IAO will ensure that a **log** is maintained of all maintenance performed on the CKDS and PFDS data sets.*

The CSFPUTIL Utility Program

- *The IAO will ensure that the* **CSFPUTIL** *utility is restricted to authorized personnel.*
- *The IAO will ensure that a* ***log*** *is maintained of all maintenance performed on the CKDS and PFDS data sets.*

ICSF Panels

- *The IAO will ensure that the ICSF ISPF data sets are protected from unauthorized access and updates. The data sets are:*

SYS3.CSF.SCSFCLI0
SYS3.CSF.SCSFPNL0
SYS3.CSF.SCSFMSG0
SYS3.CSF.SCSFSKL0
SYS3.CSF.SCSFTLIB

- *The IAO will ensure that the ICSF option in TSO is restricted to authorized personnel.*
- *The IAO will ensure that all* ***UPDATE*** *and* ***ALLOCATE*** *is logged for the ICSF Panels.*

ICSF Exits

- *The IAO will ensure that the above ICSF exits are restricted to authorized personnel.*
- *The IAO will ensure that the use of the above ICSF exits are restricted to authorized personnel and applications.*
- *The IAO will ensure that FSO reviews any GOTs exit before implementation into production.*

ICSF Event Recording

- *The IAO will ensure that ICSF events are recorded using the SMF Type 82 records and stored in the SMF data sets. Access to the SMF data sets will be restricted to authorized personnel.*

General Security Considerations

- *The IAO will ensure that the access to the in-storage copy of the CKDS is restricted to authorized personnel and applications.*
- *The IAO will ensure that CSFSERV and CSFKEYS classes have been created to perform access checking and auditing of services and keys.*
- *The IAO will ensure that the access to the CSF started task is restricted to authorized personnel and applications.*
- *The IAO will ensure that the CSF startup procedure is located in SYS1.PROCLIB.*
- *The IAO will ensure that the ICSF ISPF panels are restricted to authorized personnel.*
- *The IAO will ensure that the* ***SYS1.CSF.SCSFMOD0*** *data set is link listed.*
- *The IAO will ensure that the member* ***IKJTSO00*** *contains* ***CSFDAUTH*** *specified in the* ***AUTHPGM*** *and* ***AUTHTSF*** *sections.*
- *The IAO will ensure that ICSF services are restricted to authorized personnel and applications.*

This page is intentionally left blank.