Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepaper:

Mainframe OS/390 and z/OS Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS WHITEPAPER,* VERSION 2.0

1) Converted baseline version dated March 7, 2007 to updated CMS style format.
2) Moved Section 1, Introduction, from before Table of Contents to after.
3) Updated Section 2, Background, to add BPSSM section reference concerning the use of STIGs.
4) Added titles to the following tables:
   a) Table 1 in Section 3.12.3,
   b) Table 2 in Section 3.12.4,
   c) Table 3 in Section 3.12.7,
   d) Table 4 in Section 3.12.9, and
   e) Table 5 in Section 3.14.1.
5) Removed former Appendix A CSRs and added pointer to new CMSRs.
6) Changed CSR glossary term in Appendix B to CMSR.
7) Updated Section 3.0 and 3.5, and updated the Appendix A CMSR reference.

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS WHITEPAPER,* VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

1 INTRODUCTION

This white paper was developed by PricewaterhouseCoopers LLP (PwC) for the Centers for Medicare and Medicaid Services (CMS). This document is one of a number of white papers issued by CMS management to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment.

The intended audience of this paper however, extends beyond CMS management and staff to include all CMS business partners. In this context, a CMS business partner is any private or public sector organization which provides services to this agency. These business partners include, but are not limited to; Medicare carriers, Fiscal Intermediaries (FI), Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, claims processing data centers, Medicare Administrative Contractors (MAC), and Enterprise Data Centers (EDC).

This document is designed to provide guidance and information to CMS & CMS business partners in implementing and configuring a secure operating system (O/S). As computers and technology advanced they became capable of running several programs at once. This created a need to control resources and programs. The O/S addressed these issues by controlling the resources and functions that programs could use as well as keeping them from interfering with one another and the O/S itself.

O/S deployed by most CMS Contractor's mainframes use the International Business Machines (IBM) OS/390 or z/OS operating system package which includes the MVS O/S. The Defense Information Systems Agency (DISA), an agency of the Department of Defense (DOD), has developed an OS/390 & z/OS Security Technical Implementation Guide (STIG). The STIG, Version 5, Release 2, provides guidance on implementation of controls, configurations, and design of the OS/390 and z/OS. References within this document to OS/390 also relate to z/OS; all references to OS/390 can also be applied to z/OS.

The purpose of this document is to relay pertinent information within the STIG to CMS and applicable CMS Contractors which process information on behalf of CMS utilizing OS/390 or z/OS. Information within this document does not cover all controls and guidance provided within the STIG nor should a contractor using just this information have comfort in the overall security and integrity of their O/S. Rather, this document should be used as an introduction to the STIG and information contained within used as a starting point in developing a secure and controlled environment. This document will focus on OS/390 and z/OS Integrity and System Considerations and remote access through communication servers.

2 BACKGROUND

Federal agencies, such as CMS and CMS Contractors processing claims on their behalf, have become increasingly reliant on computerized information systems to process, maintain, and report essential information. This dependency on systems will continue to increase as technology advances and with this reliance also comes inherent vulnerabilities. Mitigating the

risks associated with computerized information processing security and controls over the systems is paramount.

A key aspect of any computerized environment is the O/S. The O/S is used to control programs and resources, allowing multiple programs to run on the mainframe without interfering with one another or the O/S. Most federal agencies process many significant transactions through the use of a mainframe and use IBM OS/390 or z/OS.

Secure configurations and controls of the O/S are essential to the integrity of a processing environment. These controls are subject to review as part of financial statement audits. Federal audit requirements applicable to the audit of CMS' financial statements include assessing the general and application controls over the processing of Medicare information and concluding on whether the controls are operating effectively.

To assist in the appropriate configuration of the O/S, DoD released the OS/390 & z/OS STIG, Version 5, Volume 2 on September 11, 2006. The STIG was developed by DISA for DoD and provides guidance for the implementation and configuration of OS/390 and the access security packages ACF2, RACF, and TSS. This document was developed with regards to the STIG and key aspects of audit work programs in order to introduce concepts provided by the STIG. The STIGs provide very useful information on establishing a control framework for the mainframe operating system. This document will relay pertinent information from the STIG to readers, however, is not a substitute for the STIG, and will not alone provide a completely secure environment. Refer to section 3.10.2 in the BPSSM concerning the use of STIGs in the business partner environment.

3 OS/390 AND Z/OS INTEGRITY AND SYSTEM CONSIDERATIONS

The IBM OS/390 and z/OS software packages contain system software for the management, administration, and (to some extent) security of an IBM mainframe computer. These packages include software utilities for system interconnectivity, batch processing, and user management and both packages include IBM's mainframe operating system called Multi-Processing Virtual Storage (MVS).

Operating systems (O/S), such as MVS, were developed and are used to control programs and resources, allowing multiple programs to run on the mainframe without interfering with one another or with the O/S. Having a centralized O/S manage the processing performed by the system provides a powerful tool. However, because not all processes, programs, and utilities should be accessible to all users on the system, the O/S needs to be controlled. To this end, hardware controls have been built into every computer running the MVS O/S. Below is a description of the three hardware controls:

CPU State (Supervisor State vs. Program State): MVS is always running in either supervisor or program state. On a mainframe, supervisor is simply another term for the O/S. When a program is operating in supervisor state it is able to execute any valid instruction, both privileged and non-privileged. When a program is in program state (sometimes referred to as 'problem' state), it can only execute non-privileged instructions. System utilities or functions, such as

altering the computer's date or controlling the computer's hardware components are not allowed. If a user or program were able to manipulate the O/S to switch to supervisory state, they would have complete control and free reign to all system utilities and data. They could inappropriately execute privileged instructions.

Protect Keys (Protection Keys/Storage Protection Key): MVS is always running in one of 16 possible protect keys (numbering 0 through 15). These keys identify additional permissions and privileges. Additionally, each piece of memory has a protect key associated with it (again, 0 through 15). When a request to execute an instruction is made, the O/S will compare the requesting memory's protect key to the current protect key MVS is running in. If the keys match, the requested instruction is executed. If the keys do not match, the instruction fails. Note: protect keys 0 through 7 are considered system keys and can bypass system security controls. If a user or program were able to manipulate the O/S to run in one of these systems keys, they could inappropriately execute privileged instructions, including switching to supervisory state without restriction from the system security software (that is, RACF, ACF2 or Top Secret Software).

Address Space: All programs running on a computer use the same physical memory, so the O/S needs a method to distinguish the memory address each program is using. Additionally, the O/S needs a method to ensure one program cannot access or override memory being used by another program. These methods are made possible through individual user translation tables and a process called Dynamic Address Translation (DAT). Each program or user has a translation table which matches the "virtual" address of data to the location of data in the physical memory or the "real" address. Because each user or program has their own translation table of the real address of their data, the O/S is able to prevent one program from even being aware of the other's data. A compromise of translation tables and appropriate address space could result in data being inappropriately disclosed or lost.

As noted, sensitive privileges can be extended by use or misuse of these controls which could lead to a compromise of system resources. By appropriately configuring MVS and implementing appropriate system controls, risks associated with the misuse of privileged hardware controls and utilities can be reduced.

To ensure the integrity of the O/S environment, the system level and data level process must be secured. The below sections will discuss some details regarding both. However, neither this document nor the STIG focus on protection of hardware devices through use of physical security controls.

The following sections will focus on risks, recommendations, and techniques for securing software integrity by means of securing the MVS O/S. The following will be discussed:

- Authorized Program Facility (APF) Libraries
- Program Properties Tables (PPT)
- Supervisor Calls (SVC)
- Time Sharing Option (TSO)
- Input/Output (I/O) Appendages

- Linklist
- Logical Parmlib
- EXITS and Intercepts
- Data set Controls

In addition, this paper will also focus on securing remote access to system resources and monitoring controls.

3.1 CONTROLLING AUTHORIZED PROGRAM FACILITY (APF) LIBRARIES

The Authorized Program Facility (APF) is a component of OS/390 and z/OS which identifies the libraries that have the ability to access special functions or programs. Those libraries are called APF authorized libraries. A library is another term for a special type of data set. Data sets are the means by which both OS/390 and z/OS manage data. The term data set refers to a file that contains one or more records. In simplest terms, a record is a fixed number of bytes containing data. A library is comprised of members and programs are stored as members of libraries. Generally, the O/S loads the members (programs) of a library into storage sequentially, but it can access members directly when selecting a program for execution. A program stored as a member of an APF library (an APF-authorized program) can do virtually anything that it wants because it is essentially an extension of the O/S. It can put itself into supervisor state or obtain a system key, it can modify system controls, it can execute privileged instructions (while in supervisor state) and it can turn off logging to cover its tracks.

A program executed in MVS is considered APF authorized if the following characteristics are met: (1) the program must be stored within and loaded from an APF Authorized Library and be linked as authorized, (AC=1) and (2) all programs that are to be subsequently loaded within the job step must also be APF authorized.

Both OS/390 and z/OS come with many standard system libraries. A system library is a data set on the system disk volume that holds control parameters for the O/S, Job Control Language (JCL) procedures, basic execution modules, and so on. The prefix SYS1.xx is used to identify system libraries, where xx is the name of library being referenced. SYS1 is the initial IBM supplied High Level Qualifier (HLQ). HLQs identify the first node of the name for a data set; however, system software may also be found within other HLQ libraries such as SYS0, SYS2, SYSx, etc. For the purposes of this document SYS1.xx will be considered the location of the libraries housing authorized programs. The data set (or library) called SYS1.PARMLIB contains control parameters for the whole system.

The list of APF authorized libraries is built at initial program load (IPL) –when the O/S is started– using data found in three sources. SYS1.PARMLIB has two members (remember that programs are stored as members of a library) named IEAAPFxx and PROGxx. The third piece of data used to build the list of APF authorized libraries is the value of the LNKAUTH setting in the SYS1.PARMLIB member IEASYSxx. A member of a library is referred to in parenthesis following the library, in this case SYS1.PARMLIB(IEASYSxx).

SYS1.PARMLIB members IEAAPFxx and PROGxx list the libraries which are APF authorized. These members both specify the names of APF authorized libraries and the volumes on which these libraries reside. However, with the PROGxx member, APF libraries can be specified as either static or dynamic. If it is static, then the list of APF-authorized libraries does not change. If it is dynamic, then APF-authorized libraries may be added or deleted by programs and by operator commands. The following is a sample entry in the IEAAPFxx member:

```
SYS1.VTAMLIB MVSRES
```

The following is how the same entry would appear in the PROGxx member:

```
APF ADD DSNAME(SYS1.VTAMLIB)          VOLUME(MVSRES)
```

The value of LNKAUTH in SYS1.PARMLIB(IEASYSxx) identifies whether libraries in the linklist are to be considered APF-authorized. The linklist is a default set of libraries that MVS searches for a specified program. The linklist libraries are listed in SYS1.PARMLIB(LNKLSTxx). If LNKAUTH is set to LNKAUTH=LNKLST, then the libraries listed in SYS1.PARMLIB(LNKLSTxx) are considered APF authorized. If LNKAUTH=APFTAB, then the linklist libraries listed in SYS1.PARMLIB(LNKLSTxx) are not considered APF-authorized. The default value for this setting is LNKAUTH=LNKLST.

The DISA STIG provides the following recommendations to ensure control over SYS1.PARMLIB and its members; please note that responsibilities delegated to the IAO (Information Assurance Officer) should be performed by an individual with appropriate knowledge and authority within the organization.

1) In SYS1.PARMLIB(IEASYSxx), use the parameter LNKAUTH=APFTAB so that all APF libraries are specified in the IEAAPFxx and PROGxx members of parmlib.

2) The IEAAPFxx and PROGxx members will contain only required libraries. On a semi annual basis, Software Support should review the volume serial numbers, and should verify them in accordance with the system catalog. Software Support will remove all non existent libraries. The IAO should modify and/or delete the rules associated with these libraries.

3) Before a library and a volume serial number are added to IEAAPFxx and PROGxx, the IAO will protect the data set from unauthorized access. Systems programming personnel will specify the requirements for users needing read or execute access to this library. Comparisons among all the APF libraries will be done to ensure that an exposure is not created by the existence of identically named modules. Address any sensitive utility concerns with the IAO, so that the function can be restricted as required. The IAO will build the appropriate protection into the ACP.

4) All update and alter access to the APF authorized libraries will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the APF authorized libraries. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

   The libraries specified in the APF list and the following additional libraries are authorized by OS/390:

   ```
   SYS1.LINKLIB
   ```

SYS1.SVCLIB

SYS1.IMAGELIB (only when accessed by the appropriate SVC)

SYS1.LPALIB (only during the IPL process)

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer will ensure that LNKAUTH=APFTAB is specified in the IEASYSxx member(s) in the currently active parmlib data set(s).
- The systems programmer will ensure that only existing libraries are specified in the APF list of libraries.
- The systems programmer and IAO will ensure that procedures are in place to review APF-authorized Libraries and are reviewed at least on a semi-annual basis.
- The IAO will ensure that Duplicate sensitive utility(ies) and/or program(s) do not exist in APF-authorized libraries.
- The IAO will ensure that Update and allocate access to all APF-authorized libraries are limited to system programmers only, unless a letter justifying access is filed with the IAO, all update and allocate access is logged.
- The IAO will ensure that update and allocate access to SYS1.LINKLIB is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.
- The IAO will ensure that update and allocate access to SYS1.SVCLIB is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.
- The IAO will ensure that update and allocate access to SYS1.IMAGELIB is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.
- The IAO will ensure that update and allocate access to SYS1.LPALIB is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, 2.1.2.1 APF.

3.1 TIME SHARING OPTION (TSO) APF AUTHORIZATION

Time Sharing Option (TSO) allows users to create an interactive session with the O/S. TSO provides a single-user logon capability and a basic command prompt interface to the O/S. Most users work with TSO through its menu-driven interface called Interactive System Productivity Facility (ISPF). ISPF is a collection of menus and panels that offers a wide range of functions to

assist users in working with data files on the system. ISPF is used by system programmers, application programmers, administrators, and others who access OS/390 or z/OS. In general, TSO and ISPF make it easier for people with varying levels of experience to interact with the MVS O/S.

Inherent in the TSO are two lists of programs that are treated by the O/S as though they are APF Authorized. In z/OS, these programs are named IKJEFTE2 and IKJEFTE8, and both modules reside in SYS1.LINKLIB. For the OS/390 environment, the programs for authorization are documented in SYS1.PARMLIB(IKJTSOxx) and in load modules IKJTABLS and IKJEFTAP, which are located in SYS1.LPALIB.

As previously mentioned, an APF-authorized program can run in supervisor state and can therefore perform any operation without the safeguards usually enforced by MVS. It is essentially an extension of the O/S because it can put itself into supervisor state or a system key. It can modify system controls, it can execute privileged instructions (while in supervisor state), and it can prevent log data from being generated on actions it performs.

The DISA STIG provides the following recommendations to ensure control over TSO APF Authorized programs; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Systems programming personnel are responsible for determining the programs required for TSO authorization by reviewing the product/program documentation.

2) Use a CMP [Change Management Program] to install and maintain any user modifications (usermods) or programs that require TSO authorization.

3) Review any programs requiring TSO authorization for potential impact to the operating environment. Provide documentation to the IAO to limit program access using sensitive utility controls.

4) Perform any user modifications or updates to the TSO authorization modules using the CMP.

5) Procedures to perform reviews of TSO authorized program(s) will exist and should be performed on a semi-annual basis.

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer and IAO will ensure that procedures are in place to review authorized TSO programs and are reviewed at least on a semi-annual basis.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.2 TSO APF Authorization.

3.1 LINKLIST

The Linklist is a default set of libraries that MVS searches to locate a specified program that has been requested for execution. This facility is used so that a user does not have to know the library names in which utility types of programs are stored. The linklist libraries are listed in the data set SYS1.PARMLIB(LNKLSTxx). The following is a portion of a sample LNKLSTxx member:

```
LNKLST DEFINE NAME (LNKLST00)

LNKLST ADD NAME(LNKLST00) DSN(SYS1.LINKLIB)

LNKLST ADD NAME(LNKLST00) DSN(SYS1.SYSB.USER.LINKLIB)
VOLUME(SYSNS3)

LNKLST ADD NAME(LNKLST00) DSN(TS.TOSSEC.CAILIB) VOLUME(S9MD05)

LNKLST ADD NAME(LNKLST00) DSN(SYS1.BCB.LIB.UTILITY) VOLUME(SYSNS1)
```

The value of LNKAUTH in the SYS1.PARMLIB(IEASYSxx) specifies whether or not linklist libraries are to be considered APF authorized. If LNKAUTH=LNKLST, then the libraries listed in SYS1.PARMLIB(LNKLSTxx) are considered APF authorized. If LNKAUTH=APFTAB, then the linklist libraries listed in SYS1.PARMLIB(LNKLSTxx) are not considered APF-authorized. This is important because the default value for this setting is LNKAUTH=LNKLST.

When set to LNKLIST, the libraries listed in SYS1.PARMLIB(LNKLIST are APF-authorized only if programs are located through system search, as opposed to JOBLIB/STEPLIB allocation. If set to APFTAB, the libraries are APF-authorized even if JOBLIB/STEPLIB is used to allocate them.

The DISA STIG provides the following recommendations to ensure control over the Linklist libraries; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Avoid inclusion of sensitive libraries in the LNKLSTxx member unless absolutely required.

2) The LNKLSTxx and PROGxx (LNKLST entries) members will contain only required libraries. On a semi annual basis, Software Support should review the volume serial numbers, and should verify them in accordance with the system catalog. Software Support will remove all non existent libraries. The IAO should modify and/or delete the rules associated with these libraries.

3) Before a library is added to LNKLSTxx, the IAO will protect the data set from unauthorized access. Systems programming personnel will specify the requirements, for which users need read or execute access to this library. Comparisons among all the Linklist libraries will be done to ensure that an exposure is not created by the existence of identically named modules. Address any sensitive program concerns to the IAO so that the function can be restricted as required. The IAO will build the appropriate protection into the ACP.

4) All update and alter access authority to Linklist libraries are logged using the ACP's facilities. Only systems programming personnel are authorized to update the Linklist

libraries. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer will ensure that only existing libraries are specified in the Linklist list of libraries.
- The systems programmer and IAO will ensure that procedures are in place to review Linklisted Libraries and are reviewed at least on a semi-annual basis.
- The IAO will ensure that update and allocate access to LINKLIST libraries is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.9 Linklist.

3.2 LOGICAL PARMLIB

A Parameter Library (PARMLIB) is a dataset within the mainframe operating system that contains parameter settings. The most important of these libraries is the SYS1.PARMLIB, which contains parameters for the operating system itself. Whenever the system is IPL'd, the parameters within PARMLIB are read in a certain sequence by the nucleus initialization program. Anyone who can change the system parameters can make changes to add uncontrolled libraries to the APF list which could bypass the system controls. They could eliminate certain audit trails or negate security mechanisms.

The DISA STIG provides the following recommendation to ensure control over the SYS1.PARMLIB; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The IAO will implement controls to specify the valid users authorized to update the SYS1.PARMLIB concatenation. (Refer to the specific Access Control Product section regarding data set access controls.)
2) All update and alter access to libraries in the concatenation will be logged using the ACP's facilities.
3) Only systems programming personnel will be authorized to update the SYS1.PARMLIB concatenation.
4) The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For

additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that update and allocate access to SYS1.PARMLIB is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.11 Logical Parmlib.

3.3 PROGRAM PROPERTIES TABLE

The Program Properties Table (PPT) is a list of programs that have been granted special properties and privileges above those that are normally permitted by the O/S. IBM includes a number of PPT entries with MVS by default, however; users are able to modify these table entries and add new ones specific to their environment. IBM supplied PPT entries can be found in LPALIB, LOAD module IEFSD060, CSECT IEFSDPPT. User-defined PPT entries can be found in SYS1.PARMLIB(SCHEDxx).

Programs listed in the PPT can be defined to receive the following special properties:

- Bypass Password Protection: Indicates whether the program is authorized to bypass password protection checking when accessing data sets protected by a password or the system's security software.
- Storage Protection Key (Protect Key): Indicates the storage protection key the program should be assigned at runtime. A protection key of less than 8 (keys 0-7), will allow a program to bypass system security controls (if the program is executed from an APF library).

Appendix C - Default Values for Sample Program Properties Table (PPT) shows the standard values for a sample PPT, as provided by IBM. If IBM-supplied modules on the system do not have the same standard values as those indicated in this appendix (or other appropriate IBM manual), then the modules could affect system integrity. Please note that a module is the object that results from compiling source code. To be ran a module must be bound to a program.

The DISA STIG provides the following recommendations to ensure control over PPT; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) As part of standard MVS maintenance, systems programming personnel will review the IEFSDPPT module and all programs that IBM has, by default, placed in the PPT to validate their applicability to the execution system. Appendix B, Sample Program Properties Table (PPT) [Appendix B within the DISA STIG], shows the standard values for a sample PPT, as provided by IBM in module IEFSDPPT for MVS/ESA, Version 4.

    - Modules for products not in use on the system will have their special privileges explicitly revoked. Do this by placing a PPT entry for each module in the SYS1.PARMLIB(SCHEDxx) member, specifying no special privileges. The PPT entry for each overridden program will be in the following format, accepting the default (unprivileged) values for the sub parameters:

PPT PGMNAME(<program name>)

The Software Support team will assemble documentation regarding these PPT entries, and the IAO will keep it on file. Include the following in the documentation:

- The product and release for which the PPT entry was made
- The last date this entry was reviewed to authenticate status
- The reason the module's privileges are being revoked

2) Systems programming personnel will review any additional module to be placed in the PPT to validate its requirements. Use the SYS1.PARMLIB(SCHEDxx) member for all programmer PPT entries. The Software Support team will assemble documentation regarding the PPT attributes. The IAO will keep this documentation on file. It will include the following:
   - The product and release for which the PPT entry is made
   - The file name in which this module resides
   - The parameter(s) requiring that this be a PPT entry (e.g., NOPASS, NOSWAP)
   - The last date this entry was reviewed to authenticate its need
   - A reference to the documentation that further explains the requirement that this be a PPT entry (i.e., the specific product installation manual)
3) Implement security controls to ensure that only authorized personnel can update the following:
   - The library where the IEFSDPPT module resides (SYS1.LINKLIB)
   - The library where the SCHEDxx member resides (SYS1.PARMLIB)
4) All update and alter access to libraries containing programs specified in the PPT will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the libraries containing programs specified in the PPT. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer and IAO will ensure that procedures are in place to review PPT entries and are reviewed at least on a semi-annual basis.
- The systems programmer will ensure that any invalid entries in the PPT via IEFSDPPT module or invalid entries in the SCHED PPT are nullified by (a) nullifying the invalid IEFSDPPT entry ensuring that there is a corresponding SCHED entry which confers no special attributes, or (b) removing the SCHED PPT entry which is no longer valid if it only exists in this member.

- The IAO will ensure that documentation for each module contained in the PPT is available.
- The IAO will ensure that update and allocate access to libraries containing PPT modules is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.3 PPT.

3.4 SUPERVISOR CALLS (SVCS)

Supervisor Calls (SVCs) are machine level instruction routines that communicate directly with the O/S to initiate, interrupt and request sensitive services for a program. Examples of services requested by an SVC include the following; I/O operations, data set allocation, file open/close, change of program status, etc. An interrupt is an event that alters the sequence in which the processor executes instructions. An interrupt might be planned (specifically requested by the currently running program) or unplanned (caused by an event that might or might not be related to the currently running program). An interrupt occurs when a program issues an SVC to request a particular system service. An SVC interrupts the program being executed and passes control to the supervisor so that it can perform the service. Programs request these services through macros such as OPEN (open a file), GETMAIN (obtain storage), or WTO (write a message to the system operator). Some SVCs are supplied with the operating system, and others are defined by the programs installed on the system. SVCs can be set to run in authorized or unauthorized state.

The IEASVCxx member of SYS1.PARMLIB specifies the numbers of user-supplied SVCs. Each SVC is specified with a number, a numeric type, and an APF value. SVCs 0-199 are reserved from IBM, SVCs numbers 200 and greater are reserved for user SVCs. However, an individual could still insert a user SVC below number 200. If APF is specified as yes, then only APF-authorized programs may issue the SVC. The name of the SVC module is derived from the number and type and the type has no security significance. The following is sample line from SYS1.PARMLIB(IEASVCxx):

- SVCPARM 225,REPLACE,TYPE(4),APF(NO)

The risk posed by SVCs is that all SVC code runs in Supervisor State and in this state the computer can execute any instruction. Accordingly, unauthorized use of SVCs can seriously affect system security, availability, and integrity and must be controlled.

The DISA STIG notes that it is essential that all SVCs not provided by IBM with the MVS operating system are analyzed for integrity exposures. Each SVC provided by a third party or written locally should be examined to determine (1) its abuse potential, (2) whether any validity checking is being performed, and (3) the steps necessary to ensure protection.

The DISA STIG provides the following recommendations to ensure control over SVCs; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Systems programming personnel will review all SVCs on a semi-annual basis to confirm that the SVCs are required and correctly installed.

2) Correct any deficiencies with an SVC, coordinating with the provider of the SVC.

3) All update and alter access to the following libraries containing SVCs will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the libraries containing SVCs. Software Support will document all the requirements for a particular SVC. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

   SYS1.SVCLIB

   SYS1.NUCLEUS

   SYS1.LPALIB

   SYS1.LINKLIB

   Any library defined in the LPALSTxx member of SYS1.PARMLIB

4) SVCs that combine both sensitive and non sensitive functions shall include protection mechanisms to ensure that sensitive functions are adequately restricted. These protection mechanisms can include, but are not limited to, the use of the TESTAUTH macro.

5) The IAO and the systems programming staff are to be aware of products that dynamically install their SVCs as part of product initialization, rather than including them in the SVC table definition.

6) The IBM manual, OS/390 MVS Planning: Security, GC28 1439, Chapter 5, lists many common errors made in coding user (i.e., non IBM supplied) SVCs. These common mistakes can present serious exposures to OS/390 integrity.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer and IAO will ensure that procedures are in place to review SVCs and are reviewed at least on a semi-annual basis.
- The IAO will ensure that SVCs are documented and registered.
- The IAO will ensure that update and allocate access to SYS1.NUCLEUS is limited to system programmers only, unless a letter justifying access is filed with the IAO, and all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, 2.1.2.4 SVCs.

3.5 INPUT/OUTPUT (I/O) APPENDAGES

An appendage is a routine or set of related instructions that provides additional control over Input/Output (I/O) operations. I/O refers to the basic operation performed by most operating systems, namely the movement of data between system devices (printer, tape drive, hard disk

drive, etc.). I/O appendages can examine the status of I/O operations and determine the actions to be taken for various conditions.

An appendage may receive control in a variety of cases. Appendages receive control in supervisor state from the system EXCP processor (the operating system macro call to initiate an I/O). To be available to non-privileged programs, appendages must be members of either the SYS1.LPALIB or SYS1.SVCLIB data sets, and must be defined in the IEAAPPxx member of SYS1.PARMLIB. Appendages have the potential to circumvent or disable system security controls, to modify audit trails, or to modify other data despite the presence of access control software.

The DISA STIG provides the following recommendations to ensure control over I/O Appendages; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The IEAAPPxx member should only contain valid I/O appendages required by unauthorized application programs. Software Support should remove appendages from IEAAPPxx when unauthorized programs no longer need them. Systems programming personnel should review all I/O appendages to confirm that the appendages are required and are correctly installed.

2) Before I/O appendages are installed in the system libraries and added to IEAAPPxx, the IAO should verify that a valid requirement for their inclusion exists.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer and IAO will ensure that procedures are in place to review I/O appendages and are reviewed at least on a semi-annual basis.
- The IAO will ensure that I/O appendages are properly documented or removed from the system.
- The IAO will ensure that documentation of I/O appendages is maintained.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.5 I/O Appendages.

3.6 EXITS AND INTERCEPTS FOR OS/390 AND SYSTEM PRODUCTS

An EXIT is a piece of code that, if executed, stops a program running, typically handing control back to the O/S for exception handling. A user EXIT is a routine that takes control at a specific point in an application. User EXITS are often used to provide additional initialization and termination functions.

OS/390 and many other products provide EXITS that can be used to perform additional processing for an installation. Examples of such products and programs are SMF, JES2, TSO, ISPF, CICS, OMEGAMON, and SDSF, to name a few. Many exits have the potential to open

integrity exposures since the code may be entered in an authorized state. Every EXIT point used within a product (especially MVS) or written by a user needs to be validated so the code does not bypass the integrity of the operating environment. eTrust CA-EXAMINE is a MVS software package that can be used to automatically assemble a list of all product exits.

The capability to perform dynamic EXIT maintenance was introduced as an inherent feature of MVS/ESA, Version 5, Release 1. This mechanism is controlled by the CSVDYNEX macro, the SYS1.PARMLIB(PROGxx) member, the SET PROG=xx command, and the SETPROG EXITS command.

The command SET PROG=xx dynamically changes the EXIT definitions based on the information in the specified PROGxx member. The SETPROG EXITS command provides the capability to selectively add and delete EXIT routines from EXIT definitions.

The DISA STIG provides the following recommendation to ensure control over EXITS; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Document all exit points used. Provide this to the IAO for backup documentation purposes.
2) Using the ACP, protect the data sets associated with all product exits installed in the OS/390 environment. This reduces the potential of a hacker adding a routine to a library and possibly creating an exposure.
3) Track all exits using a CMP [Change Management Product]. Develop usermods to include the source/object code used to support the exit.
4) Systems programming personnel will review all OS/390 and other product exits to confirm that the exits are required and are correctly installed.
5) All update and alter access to libraries containing OS/390 and other system level exits will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the libraries containing OS/390 and other system level exits. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that documentation of all installed OS/390 and other product exits are kept on file.
- The IAO will ensure that update and Allocate access to Libraries containing EXIT modules is limited to system programmers only, unless a letter justifying access is filed with the IAO, all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.6 OS/390 and Other Product Exits.

3.7 ACCESS CONTROL PRODUCT EXITS

In regards to EXITS the ACPs themselves, RACF, ACF2, and TSS, can present some of the greatest exposures. Each ACP allows installation EXIT points that can be used to support additional security-related requirements for a site. One example of such an EXIT is a password validation EXIT program restricting the contents of a password.

The DISA STIG provides the following recommendation to ensure control over ACP exits; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The site DAA [Designated Approving Authority] approves the use of any ACP exit. Use of any exit without this approval is prohibited. All code will be provided to an independent, knowledgeable, and authorized individual for review.

   Please note that the DAA should be considered an individual with the appropriate knowledge and authority to approve and EXIT, such as a system owner.

2) An authorized and independent individual with appropriate knowledge reviews the exit for use and integrity, and evaluates the need for such an exit across all OS/390 platforms. If deemed a viable process, steps are taken to prepare the exit for distribution to applicable sites.

3) Systems programming personnel reviews all ACP exits to confirm that the exits are required and are correctly installed.

4) All update and alter access to libraries containing ACP exits will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the libraries containing ACP exits. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that Documentation of all installed OS/390 and other product exits are kept on file.
- The IAO will ensure that approved documentation of additional system exits, SVCs. I/O appendages, PPT privileges, and APF authorization is on file to preserve the integrity of the Operating System.
- The IAO will ensure that update and Allocate access to Libraries containing EXIT modules is limited to system programmers only, unless a letter justifying access is filed with the IAO, all update and allocate access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.7 Access Control Product Exits.

3.8 SYSTEM DATA SET CONTROLS

Data set integrity is a key factor in the protection of MVS systems. The DISA STIG recommends protecting the following critical system data sets including, but not limited to, the following:

- System catalogs (Master Catalog and User Catalogs)
- System libraries:
  - OS/390 libraries (e.g., Linklist, LPA, SVC, parmlib concatenation, IODF [Input/Output Definition File])
  - System-level product libraries (e.g., CA-1)
  - OS/390 and product installation libraries (e.g., the SMP/E CSI, DLIBs)
- Access Control Product files and databases
- JES2 SPOOL file (SYS1.HASPACE)
- JES2 SPOOL checkpoint file (SYS1.HASPCKPT)
- User attribute data set (SYS1.UADS)
- SMF data files (SYS1.MANx)
- System and subsystem trace data sets (e.g., GTF, OS/390 Component Trace)
- System dump data sets (SYS1.DUMPxx)
- Logs
- Backups, dumps, and off-loads of the above (e.g., JES2 SPOOL off-loads, external writer output from SYSLOG, SMF dumps, system DASD dumps)
- System page data sets (PLPA, COMMON, and LOCAL)
- Parameter

The DISA STIG states that control restrictions should be enforced for these files to ensure that (1) only those routines or users with a legitimate need are granted access, and (2) the access granted is restricted to the minimum level necessary.

The DISA STIG provides the following techniques which note the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that update and allocate access to JES2 System datasets (spool, checkpoint, and Parmlib datasets) are limited to system programmers only, unless a letter justifying access is filed with the IAO.

- The IAO will ensure that allocate access to SYS1.UADS is limited to system programmers only, read and update access to SYS1.UADS is limited to system programmer personnel and/or security personnel, unless a letter justifying access is filed with the IAO, and all dataset access is logged.
- The IAO will ensure that update and allocate access to SYS1.DUMP data set(s) is limited to system programmers only, unless a letter justifying access is filed with the IAO.
- The IAO will ensure that update and allocate access to System backup files is limited to system programmers and/or batch jobs that perform DASD backups, unless a letter justifying access is filed with the IAO.
- The IAO will ensure that update and allocate access to SYS1.TRACE is limited to system programmers only, unless a letter justifying access is filed with the IAO.
- The IAO will ensure that update and allocate access to SYSTEM PAGE datasets (i.e., PLPA, COMMON, and LOCALx) is limited to system programmers only, unless a letter justifying access is filed with the IAO.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.3.1 Data Set Integrity.

3.9 REMOTE ACCESS TO SYSTEM RESOURCES – COMMUNICATION SERVERS

The ability to remotely access a z/OS or OS/390 system poses additional security risks that need to be addressed. This section focuses on two communications services inherent in the z/OS and OS/390 environments, specifically, File Transfer Protocol (FTP) Server and Telnet Server. The sections which follow contain information taken directly from the DISA STIG which includes explanations of FTP and Telnet, and controls (recommendations and techniques) surrounding FTP and Telnet. Please note that the information provided does not consist of all controls presented by the STIG and should not be considered a substitute for the STIG.

3.10 FTP SERVER

The File Transfer Protocol (FTP) Server component of IBM's Communications Server provides the server portion of the client / server application for transferring files between hosts. Because the server implements the industry standard File Transfer Protocol on OS/390, standards compliant clients running on any other host can connect to the server. Please note that FTP normally listens for connections on port 23.

It should be noted that the information in this section has been prepared to address the configuration requirements as of Version 2, Releases 8 and 10 of OS/390. IBM fundamentally altered the FTP Server component in OS/390 Version 2, Release 5, to utilize OS/390 UNIX System Services. That architecture, with enhancements, is used in the current releases of Communications Server.

The tasks supported by the FTP Server can be grouped into three categories:

- Standard functions that support transferring data and navigating the server's file systems.
- Standard functions beyond the scope of data transfer. These include renaming files, deleting files, and changing account passwords.
- OS/390-specific functions including interfacing with JES2 and DB2.

From a high level point of view, the FTP Server consists of the following elements:

- The FTP daemon program (FTPD) performs initialization and listens for incoming client connections.
- The FTP server program (FTPDNS) is executed once for each client connection and processes the client's commands until the connection is terminated.

A daemon is a program that runs unattended to perform continuous or periodic functions, such as network control. A daemon is typically started during system load and runs continuously unless terminated by a system administrator or automatically at shut down. It handles service requests of various kinds within the O/S environment and from the network. When the FTP daemon is started, it processes the configuration files and verifies that communications with the TCP/IP communications stack is available. In default configurations the daemon's address space has a job name of FTPD.

After initialization is complete, the FTP daemon creates a new address space that executes the daemon, listening for client connection requests. The original address space terminates. In default configurations the new daemon address space has a job name of FTPD1.

Each time the FTP daemon receives a connection request, it starts a new FTP server process with its own corresponding address space. Each active FTP session requires an instance of the FTP server program. In default configurations the server address space initially has a job name of FTPDn, where the n is a number 1 through 9.

The FTP server program performs identification and authentication of the client, switches its security context to that of the client, and then processes the commands sent from the client. Following successful client authentication, the job name of the server's address space is changed by default to match the user identification supplied by the client. When the client terminates the connection, the server program terminates and its corresponding address space is cleared.

The job names assigned to the various address spaces are based on OS/390 UNIX defaults. The use of an eight-character startup JCL procedure can change the default behavior.

There are a number of configuration issues relative to the security environment for the FTP Server. The following issues are addressed in the next subsections:

- Startup procedure choices and parameters
- Configuration files
- Configuration statements in the FTP.DATA file
- User exits
- Banner message requirements

- SMF recording
- Interface to JES2
- Interface to DB2

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4 FTP Server.

3.10.1 STARTUP PROCEDURE CHOICES AND PARAMETERS

There are multiple ways to start the FTP daemon. It can be started through the AUTOLOG subtask in the TCPIP address space, through an OS/390 started task, or through a command in the /etc/rc file in the OS/390 UNIX environment.

All IP applications on OS/390 and z/OS require the TCP/IP to be running in order for IP communications to occur. Automated IP application monitoring is the process that allows TCP/IP to start these applications and monitor them to make sure they continue to run correctly. The AUTOLOG statement contains a list of started task names that should be started and remain functional while TCP/IP itself is running. To determine if an application is functional, TCP/IP checks periodically to see if the process's address space and assigned ports are active. If either the assigned ports or address space is not active, TCP/IP restarts the process. By default, TCP/IP checks every five minutes for an active listen.

If, for example, an organization wanted to have the FTP server automatically started and monitored every five minutes by the TCP/IP task, the following entry would be made in PROFILE.TCPIP:

```
AUTOLOG 5

FTPD JOBNAME FTPD1

ENDAUTOLOG

PORT

20 TCP OMVS NOAUTOLOG

21 FTPD1
```

When the FTP daemon is started through the AUTOLOG subtask or through an OS/390 started task, a conventional JCL procedure (PROC) is used (as shown above). Using a PROC enhances security because it enables the explicit specification of job name, program parameters, and configuration files.

The FTP daemon program can accept parameters in the JCL procedure used to start the daemon. The ANONYMOUS and ANONYMOUS= keywords are designed to allow anonymous FTP connections. The INACTIVE keyword is designed to set the timeout value for inactive connections. Controlling these options through the configuration file statements rather than the start-up parameters reduces ambiguity.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS [Internet Connection Sharing] will ensure that the FTP daemon runs under its own user account. Specifically, it does not share the account defined for the OS/390 UNIX kernel.
- The systems programmer responsible for supporting ICS will ensure that the startup parameters for the FTP daemon does not include the ANONYMOUS, ANONYMOUS=, or INACTIVE keywords.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.1 Startup Procedure Choices and Parameters.

3.10.1 CONFIGURATION FILES

The FTP Server components read two configuration files that contain operational parameters. Because system security is impacted by some of the parameter settings, the files themselves should be protected and certain parameter settings should be specified. The first configuration file is referred to as the TCPIP.DATA file. The second configuration file is referred to as the FTP.DATA file. During initialization the FTP daemon searches multiple locations for the TCPIP.DATA and FTP.DATA files. However, uncertainty is reduced and security auditing is enhanced by explicitly specifying the locations of the files. In the daemon's started task JCL, Data Definition (DD) statements can be used to specify the locations of the files. The SYSTCPD DD statement identifies the TCPIP.DATA file and the SYSFTPD DD statement identifies the FTP.DATA file.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that the FTP daemon's started task JCL specifies the SYSTCPD and SYSFTPD DD statements for configuration files.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.2 Configuration Files.

3.10.1 FTP.DATA CONFIGURATION STATEMENTS

The statements in the FTP.DATA configuration file specify the parameters and values that control the operation of the FTP Server components. Several of the parameters should have specific settings to provide a secure configuration.

A short sample of an FTP.DATA file is shown below. Note that any configuration statements not defined are assigned default values.

```
BANNER /etc/ftp.banner

ANONYMOUSLEVEL 3
```

ANONYMOUSFILEACCESS HFS

FTPLOGGING TRUE

STARTDIRECTORY HFS

The DISA STIG states that the systems programmer responsible for supporting ICS will ensure that the FTP Server FTP.DATA configuration statements are coded according to the settings in the following table:

Table 1 FTP.DATA Configuration Statements

FTP.DATA Configuration Statements	
Statement	Not Coded, Coded without Value, or Parameter Value
ANONYMOUS	[Not Coded]
BANNER [For OS/390 2.10 and later]	[An HFS file, e.g., /etc/ftp.banner, or an OS/390 data set]
INACTIVE	[A value between 1 and 900]
JESINTERFACELEVEL [For OS/390 2.10 and later]	1 [See Note 1]
SMF	STD
SMFAPPE	[Not Coded]
SMFDEL	[Not Coded]
SMFEXIT	[Not Coded]
SMFJES	[Coded without Value]
SMFLOGN	[Not Coded]
SMFREN	[Not Coded]
SMFRETR	[Not Coded]
SMFSQL	[Coded without Value]
SMFSTOR	[Not Coded]
UMASK	077 [See Note 2]
Note: The JESINTERFACELEVEL statement may be coded with a value of 2 if the appropriate SAF resources (in the JESSPOOL and SDSF classes) have been protected. See section below entitled Interface to JES for information. Note: If the FTP Server requires a UMASK value less restrictive than 077, requirements should be justified and documented with the IAO.	

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.3, FTP.DATA Configuration Statements.

3.10.2 USER EXITS

There are a number of user EXIT points in the FTP Server component that permit customization of its operating behavior. The following table lists the EXITS with a brief description of their function:

Table 2 FTP Server User EXIT Points

FTP Server User EXITS	
EXIT Name	Function
FTCHKCMD	Control which FTP commands a user is allowed to use
FTCHKIP	Control which client hosts, by IP address, may connect to the FTP server
FTCHKJES	Control which users are allowed to submit batch jobs
FTCHKPWD	Control which users are allowed to log on to the FTP server
FTPOSTPR [For OS/390 2.10 and later]	Perform post processing tasks (such as writing syslog messages) following the completion of some FTP commands
FTPSMFEX	Perform modifications to SMF records

The FTPSMFEX EXIT is enabled when the SMFEXIT parameter is coded in the FTP.DATA configuration file. The remaining exits are enabled when their load modules are in the FTP daemon's STEPLIB or in the system link list or link pack area (LPA). The data sets in which the exits reside should be APF-authorized and program controlled.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that the FTP Server user exits are not implemented.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.4, User Exits.

3.10.3 WARNING BANNER

As of OS/390 Release 2.10, the FTP Server supports the display of a message immediately after a new connection is established. The FTP.DATA BANNER parameter controls this behavior.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that for systems at OS/390 Release 2.10 and above, the FTP.DATA BANNER parameter specifies an HFS file or OS/390 data set that contains the warning logon banner.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.5 Warning Banner.

3.10.4 SMF RECORDING

The FTP Server can provide audit data in the form of SMF records. SMF record type 118, the TCP/IP Statistics record, can be written with the following subtypes:

70 – Append

71 – Delete and Multiple Delete

72 – Invalid Logon Attempt

73 – Rename

74 – Get (Retrieve) and Multiple Get

75 – Put (Store and Store Unique) and Multiple Put

SMF data produced by the FTP Server provides transaction information for both successful and unsuccessful FTP commands. This data may provide valuable information for security audit activities.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that the FTP Server is configured to write SMF records for all eligible events.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.6 SMF Recording.

3.10.5 INTERFACE TO JOB ENTRY SUBSYSTEM (JES)

The FTP Server provides an interface to the Job Entry Subsystem (JES) that allows an FTP client to submit, retrieve, and delete jobs as well as listing their status. The interface is enabled for an FTP connection when the FILETYPE JES parameter is specified in the FTP.DATA configuration file or when the FTP client issues a SITE FILETYPE=JES command.

In OS/390 Release 2.8 the FTP client is restricted to listing, retrieving, or deleting only held jobs with names that match their logged in client ID plus one character.

As of OS/390 Release 2.10, the FTP Server's interface to JES2 has been enhanced to permit significantly more client access. With this additional access come additional risks that need to be controlled. By default the behavior of prior releases is maintained. When the JESINTERFACELEVEL parameter in the FTP.DATA configuration file is set to the value 2, the enhanced support is activated. The additional access is enabled through new commands and is controlled through resources in existing System Authorization Facility (SAF) classes.

With JESINTERFACELEVEL 2, access to JES data is controlled at two levels. The first level involves filtering criteria. Users can be given access to SAF resources that allow them to issue commands to alter the filtering criteria. The second level involves the retrieval or deletion commands. Users can be given read access to SAF resources to allow them to retrieve JES data or alter access to those resources to allow them to retrieve or delete JES data.

The SAF resources that control the filtering commands are subsets of those defined for the System Display and Search Facility (SDSF) product. The resources that control the retrieval and deletion commands are those defined for JES SPOOL data. The following table summarizes the SAF resources, the class they belong to, and the associated FTP client commands:

Table 3 FTP Server JES Interface SAF Resources

FTP Sever JES Interface SAF Resources		
SAF Resource	SAF Class	Client Commands
nodeid.userid.jobname.jobid.Dsid.dsname	JESSPOOL	DELETE, MDELETE
nodeid.userid.jobname.jobid.Dsid.dsname	JESSPOOL	GET, MGET
ISFCMD.FILTER.PREFIX	SDSF	JESJOBNAME, GET, MGET, DIR, LIST
ISFCMD.FILTER.OWNER	SDSF	JESOWNER, GET, MGET, DIR, LIST
ISFCMD.DSP.INPUT.jesx ISFCMD.DSP.ACTIVE.jesx ISFCMD.DSP.OUTPUT.jesx where jesx is the Job Entry Subsystem name (e.g., JES2)	SDSF	JESSTATUS, LIST, NLIST

The JESJOBNAME, JESOWNER, and JESSTATUS commands are actually subcommands of the client SITE command. They set up filtering criteria as follows:

JESJOBNAME limits data based on the name of the job.

JESOWNER limits data based on the ID of the owner of the job.

JESSTATUS limits data based on the JES queue status of the job. This status can be INPUT, ACTIVE, OUTPUT, or ALL.

It is apparent that control of the resources in the JESSPOOL and SDSF SAF classes is critical to maintaining security for the FTP interface to JES. However, because the interface uses resources that are already defined to secure the use of SDSF to access JES data, most sites have already taken the required steps. Information on securing the JESSPOOL class resources is discussed in the DISA OS/390 and z/OS STIG, Section 5.1.4, Security Controls for JES2 SPOOL Data Sets.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that for systems at OS/390 Release 2.10 and above, the FTP.DATA JESINTERFACELEVEL parameter is set to 1 unless the resources in the JESSPOOL and SDSF SAF classes have been protected.

Refer to IBM’s OS/390 IBM Communications Server IP Configuration Guide document for details on customizing the FTP interface to JES.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.7 Interface to JES.

3.10.6 INTERFACE TO DB2

The FTP Server provides an interface to IBM’s DB2 database management system that allows an FTP client to submit queries (via SQL SELECT) and retrieve the output. The interface is enabled for an FTP connection when the FILETYPE SQL parameter is specified in the FTP.DATA configuration file or when the client issues a SITE FILETYPE=SQL command.

To use this interface, a valid DB2 subsystem name and DB2 plan should be specified in the FTP.DATA configuration file. The FTP client may also set the DB2 subsystem name dynamically using the SITE DB2= command. IBM supplies a sample for defining and permitting access to the DB2 plan in the OS/390 IBM Communications Server IP Configuration Guide document (OS/390 Release 2.10) or OS/390 SecureWay Communications Server IP Configuration document (OS/390 Release 2.8).

Security for the DB2 interface is controlled via the DB2 access controls. These controls are typically implemented through GRANT operations. The site should ensure that only appropriate DB2 data would be made available when this interface is enabled.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.1.8 Interface to DB2.

3.10.7 HIERARCHICAL FILE SYSTEM (HFS) OBJECT PROTECTION

In order to protect the FTP Server component, special security settings are applied to selected Hierarchical File System (HFS) files. A HFS is a collection of files and directories organized in a hierarchical structure that can be accessed using z/OS UNIX System Services.

The DISA STIG states that the systems programmer should ensure that the permission bits and user audit bits for HFS objects that are part of the FTP Server component are configured according to the settings in the following table:

Table 4 FTP Server HFS Object Security Settings

FTP Server HFS Object Security Settings			
Directory or File	Permission Bits	User Audit Bits	Fucnction
/usr/sbin/ftpd	1740	fff	Daemon program
/usr/sbin/ftpdns	1755	fff	Server program
/etc/ftp.data	0744	faf	Daemon configuration file
/etc/ftp.banner	0744	faf	Connection message
Note: The /usr/sbin/ftpd and /usr/sbin/ftpdns objects are symbolic links to /usr/lpp/tcpip/sbin/ftpd and /usr/lpp/tcpip/sbin/ftpdns respectively. The permission and user audit bits on the targets of the symbolic links should have the required settings. Note: The /etc/ftp.data file may not be the configuration file the server uses. It is necessary to check the startup PROC to determine the actual file. Note: The etc/ftp.banner file may not be the banner file the server uses. It is necessary to check the configuration file to determine the actual file.			

Some of the files listed above (e.g., /etc/ftp.data) are not used in every configuration. While the absence of a file is generally not a security issue, the existence of a file that has not been properly secured can often be an issue. Therefore, all files that do exist should have the specified permission and audit bit settings.

The following commands can be used (from a user account with an effective UID(0)) to update the permission bits and audit bits:

```
chmod  1740  /usr/lpp/tcpip/sbin/ftpd

chaudit  rwx=f  /usr/lpp/tcpip/sbin/ftpd
```

```
chmod  1755  /usr/lpp/tcpip/sbin/ftpdns
chaudit  rwx=f  /usr/lpp/tcpip/sbin/ftpdns
chmod  0744  /etc/ftp.data
chaudit  w=sf,rx+f  /etc/ftp.data
chmod  0744  /etc/ftp.banner
chaudit  w=sf,rx+f  /etc/ftp.banner
```

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.4.2 HFS Object Protection.

Please note that the DISA STIG offers additional guidance in regards to FTP and in regards to ACP and FTP.

3.11 TELNET SERVER

The Telnet Server provides the server portion of the client/server application that allows interactive terminal access from clients on TCP/IP networks to applications on an OS/390 or z/OS host. Transmission Control Protocol/Internet Protocol (TCP/IP) is an industry-standard, nonproprietary set of communications protocols that provides reliable end-to-end connections between applications over interconnected networks of different types. TCP/IP was widely embraced when the Internet came of age because it permitted access to remote data and processing for a relatively small cost. TCP/IP and the Internet resulted in a proliferation of small computers and communications equipment for chat, e-mail, conducting business, and downloading and uploading data. A Telnet Server listens for TCP/IP connection requests from clients and sends host data back to the clients.

A Telnet Server also sends data to and receives data from SNA applications. System Network Architecture (SNA) was developed by IBM. SNA enabled corporations to communicate among its locations around the country. To do this, SNA included products such as Virtual Telecommunication Access Method (VTAM), Network Control Program (NCP) and terminal controllers as well as the synchronous data link control (SDLC) protocol. What TCP/IP and the Internet were to the public in the 1990s, SNA was to large enterprises in the 1980s.

It should be noted that the information in this section has been prepared to address the configuration requirements as of Version 2, Releases 8 and 10 of OS/390. IBM made significant changes to the software between these releases and parameter differences reflect these changes. Please refer to the OS/390 IBM Communications Server IP Configuration Guide document (OS/390 Release 2.10) or the OS/390 SecureWay Communications Server IP Configuration document (OS/390 Release 2.8) for documentation of specific syntax.

The configuration issues addressed relative to the security environment for the Telnet Server include the following:

- Configuration statements in the PROFILE.TCPIP file
- Controlling session setup

- Banner message requirements
- Secure Sockets Layer (SSL) connections
- SMF recording

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2 TN3270 Telnet Server.

3.11.1 PROFILE.TCPIP CONFIGURATION STATEMENTS

The Telnet Server uses configuration statements in the file referred to as the PROFILE.TCPIP file. Because system security is impacted by some of the parameters in the PROFILE.TCPIP file, and the default settings do not provide an adequate level of security, certain parameter settings should be explicitly specified. Those required parameter settings are discussed in this section.

The Telnet Server is capable of listening to up to 255 IP ports. The Internet Assigned Numbers Authority (IANA) defines two ports for Telnet in the range of well known ports. Port 23 is assigned to common Telnet connections; port 992 is assigned to Telnet protocol over TLS/SSL (a security protocol that provides communication privacy). Different ports are used as a simple mechanism to allow connections with different operating characteristics to coexist. Accordingly, the Telnet Server configuration statements are organized into statement blocks to allow different ports to be assigned different parameter values.

The configuration statements for the Telnet Server are expressed in two statement blocks in OS/390 Release 2.8 and three blocks in Release 2.10:

TELNETGLOBALS (OS/390 Release 2.10): Includes parameters that apply to all ports.

TELNETPARMS: Includes parameters that define the characteristics of one port.

BEGINVTAM: Includes parameters that define characteristics related to VTAM, such as Logical Unit (LU) names and application relationships.

While there may only be one TELNETGLOBALS block (OS/390 Release 2.10) in the PROFILE.TCPIP file, the number of TELNETPARMS blocks corresponds directly to the number of ports to which the server is listening. BEGINVTAM blocks can correspond to one or more TELNETPARMS blocks, depending on the parameters to be applied. For example, if the site intends for the server to listen to ports 23 and 992, there is one TELNETGLOBALS block (OS/390 Release 2.10), two TELNETPARMS blocks, and one or two BEGINVTAM blocks. The requirements in this section are documented to correspond to this structure.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.1 PROFILE.TCPIP Configuration Statements.

3.11.1.1 TELNETGLOBALS STATEMENTS

The TELNETGLOBALS block is used in OS/390 Release 2.10 to supply parameters that apply to all TELNETPARMS blocks. The KEYRING statement can be coded once in the TELNETGLOBALS block rather than multiple times in TELNETPARMS blocks. KEYRING

specifies the source for digital certificates required for Telnet SSL processing. Since all ports that are supporting SSL processing should use the same KEYRING file, it reduces ambiguity to have it coded in one place. The Telnet Server in OS/390 Release 2.10 allows the use of an MVS data set, an HFS file, or the resident ACP as the source for digital certificates. Use of the ACP is consistent with the security philosophy maintained for OS/390 systems.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that for systems at OS/390 Release 2.10 and above, the KEYRING statement, if used, is only coded within the TELNETGLOBALS statement block and specifies the SAF parameter, indicating that the resident ACP manages the digital certificates being used.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.1 PROFILE.TCPIP Configuration Statements.

3.11.1.1 TELNETPARMS STATEMENTS

Each TELNETPARMS block specifies parameters for a specific IP port. Several of these parameters have potential impacts to system security and therefore require specific settings.

PORT and SECUREPORT are mutually exclusive within a TELNETPARMS block. A PORT statement defines an IP port for basic sessions. For systems at OS/390 Release 2.8, the SECUREPORT statement defines an IP port for sessions that use the SSL protocol. For systems at OS/390 Release 2.10, the SECUREPORT statement defines an IP port for sessions that may use the SSL protocol, subject to additional configuration options.

For systems at OS/390 Release 2.8, the SECUREPORT statement includes the KEYRING operand, and it specifies the MVS data set or HFS file that is the source for digital certificates required for TN3270 SSL processing. Using an MVS data set provides enhanced security compared to an HFS file.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that for systems at OS/390 Release 2.8, the KEYRING operand on any SECUREPORT statement, if used, specifies an MVS data set as the source for digital certificates.

Defining a SECUREPORT can provide the advantages of an additional authentication mechanism and session encryption at the expense of acquiring and maintaining the required digital certificate. The following recommendations apply:

At least one TELNETPARMS block with a PORT statement and one TELNETPARMS block with a SECUREPORT statement should be defined.

Port number 23 should be specified on the PORT statement and port number 992 should be specified on the SECUREPORT statement.

Locations with systems at OS/390 Release 2.10 could define a single port, typically 23, that supports multiple types of Telnet sessions. This allows one port to support basic, SSL sessions, and negotiated SSL sessions.

The TELNETPARMS INACTIVE statement defines the terminal inactivity timeout value. When there has been no client-VTAM activity for the specified number of seconds, the session will be dropped. Note that the value of the INACTIVE parameter can impact the values of the PRTINACTIVE and KEEPINACTIVE (OS/390 Release 2.10) statements. The STIG requirement recommends that user sessions be terminated or locked out after 15 minutes of inactivity. Documentation should be maintained when this guideline is not followed.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that unless documented with the IAM, a TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900. Exceptions are documented with the IAO.

For OS/390 Release 2.10 systems, the TELNETPARMS TKOSPECLURECON statement can be used to specify that an existing, inactive session with a specific (VTAM) Logical Unit (SPECLU) name can be taken over by a client specifying that name. This capability is intended to allow existing sessions to be recovered when a network connection fails. However, the last screen displayed in the original session is re-sent without any authentication of the client. In some circumstances, this could allow one user to connect to another user's session.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that the TELNETPARMS TKOSPECLURECON statement is not coded in any TELNETPARMS statement block.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.1 PROFILE.TCPIP Configuration Statements.

3.11.1.1 BEGINVTAM STATEMENTS

Each BEGINVTAM statement block specifies VTAM session and application parameters for one or more IP ports. Several of these parameters have potential impacts to system security and therefore require specific settings.

The BEGINVTAM ALLOWAPPL and RESTRICTAPPL statements are intended to provide a level of control for access from Telnet clients to VTAM applications. The statements can also include some operating parameters that may be applicable to certain applications. Application

access control is required for unsecured terminals and is handled by session manager software. The BEGINVTAM ALLOWAPPL statement may be coded to provide operating parameters. It should not be coded with the LU or LUG (OS/390 Release 2.10) operand for the purpose of access control. Since operating parameters can be coded on ALLOWAPPL instead of RESTRICTAPPL, there is no environment where RESTRICTAPPL would be applicable.

Some special considerations apply to the following BEGINVTAM statements:

DEFAULTAPPL

HNGROUP

INTERPTCP

IPGROUP

LINEMODEAPPL

LUMAP

PARMSMAP (OS/390 Release 2.10)

PRTMAP

USSTCP

These statements can include operands that specify client source IP addresses or host names.

For IP addresses, consideration should be given to two potential issues—dynamic client IP addresses and address spoofing. The use of Dynamic Host Configuration Protocol (DHCP) or proxy firewalls can result in the same client host using different source IP addresses on successive connections. It can also result in two different client hosts using the same source IP address at different times. IP address spoofing, the unauthorized use of a legitimate IP address, results in the incorrect identification of a client. The impact of these issues is that a client IP address may not be an accurate indicator of the identity of the client.

For host names, consideration should be given to the fact that using host names requires that the Telnet Server resolve the name to an IP address. Whether name resolution is done via files or a name server, the data should be kept accurate and its integrity should be assured.

As a result of these considerations, BEGINVTAM statement operands containing IP addresses or host names should be used only when the sources for that information are considered to be trusted.

The BEGINVTAM MSG07 statement provides information to the client when a session attempt fails. When MSG07 is not used, the connection is dropped without providing an error message. Although this parameter is not directly related to security, it can provide helpful diagnostic information in cases where sessions fail due to the values of security-related parameters. In addition, some Telnet client programs may experience auto-reconnect loops when a connection is dropped without an error message. For most OS/390 images, the BEGINVTAM MSG07 statement should be coded.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that the BEGINVTAM RESTRICTAPPL statement is not coded in any BEGINVTAM statement block.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.1 PROFILE.TCPIP Configuration Statements.

3.11.2 SESSION SETUP CONTROL

After a connection from a Telnet client to the Telnet Server has been established, the process of session setup with a VTAM application occurs. A number of BEGINVTAM statements will be coded in a specific configuration to ensure that adequate control over access to VTAM applications is maintained.

Network connections can originate from secure terminals or unsecured terminals. The Telnet Server should be configured to address these two types of connections. Terminals should meet two conditions to be considered secure. One condition involves the hardware and configuration. Secure terminals include devices that are directly attached to the host, such as 3270-type terminals coax connected to a 3174 Control Unit. They also include PCs running 3270 terminal emulation clients attached to a private LAN (i.e., a LAN without access to an external network). The other condition involves the location of the terminals. Secure terminals are located in areas with physical access limited to authorized personnel. Examples of terminals that are not secure are those attached via dial-in servers. The intent of this distinction is to allow additional connection options (e.g., bypassing session manager control) to authorized personnel working in controlled access areas. These connection options may be necessary for operational control or for system recovery procedures.

The BEGINVTAM USSTCP statement can be used to specify a customized Unformatted System Services (USS) table for client connections. The USS table can provide a level of access control by restricting the commands that allow connections to VTAM applications. The USS table specified by the USSTCP statement can be the same as the one used by the SNA component of IBM Communications Server.

The BEGINVTAM DEFAULTAPPL statement can be used to specify the VTAM application to which a client is automatically connected when a session is established using a protocol other than linemode protocol.

The BEGINVTAM LINEMODEAPPL statement can be used to specify the VTAM application to which a client is automatically connected when a session is established using the linemode protocol. Because USSTCP processing does not apply to clients using the linemode protocol, the LINEMODEAPPL statement is used for application access control.

For OS/390 Release 2.10 systems, the BEGINVTAM LUMAP statement can specify a default VTAM application using the DEFAPPL operand. This processing is similar to the DEFAULTAPPL and LINEMODEAPPL processing, except that a client identifier should be

coded. When a client matches the LUMAP specification, the DEFAPPL specification overrides the DEFAULTAPPL or LINEMODEAPPL specifications.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. The named table allows access only to session manager applications and NC PASS applications. This USSTCP statement does not specify any type of client identifier, such as host name or IP address, so that the statement applies to all connections not otherwise controlled.

- The systems programmer responsible for supporting ICS will ensure that within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications are coded only if the statements include a client identifier operand that references only secure terminals.

- The systems programmer responsible for supporting ICS will ensure that any BEGINVTAM DEFAUTLAPPL statement that does not specify a client identifier, or specifies any type of client identifier that would apply to unsecured terminals, specifies a session manager application or an NC PASS application as the application name.

- The systems programmer responsible for supporting ICS will ensure that within each BEGINVTAM statement block, one BEGINVTAM LINEMODEAPPL statement is coded that specifies only the application name and, for OS/390 Release 2.10, DEFONLY operands. The named application specifies a session manager application or an NC PASS application. This LINEMODEAPPL statement does not specify any type of client identifier, such as host name or IP address, so that the statement applies to all linemode connections not otherwise controlled.

- The systems programmer responsible for supporting ICS will ensure that any BEGINVTAM LINEMODEAPPL statement that specifies any type of client identifier that would apply to unsecured terminals specifies a session manager application or an NC PASS application as the application name.

- The systems programmer responsible for supporting ICS will ensure that for systems at OS/390 Release 2.10 and above, any BEGINVTAM LUMAP statement, if used with the DEFAPPL operand and applied to unsecured terminals, specifies only a session manager application or an NC PASS application.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.2 Session Setup Control.

3.11.3 WARNING BANNER

Within the Telnet Server, a banner can be implemented through the USS table that is specified on a BEGINVTAM USSTCP statement. The text associated with message ID 10 (i.e., MSG10)

in the USS table is sent to clients that are subject to USSTCP processing.
The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that all USS tables referenced in BEGINVTAM USSTCP statements includes MSG10 text that specifies a warning logon banner.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.3 Warning Banner.

3.11.4 SSL CONNECTIONS

The Telnet Server is capable of using the Secure Sockets Layer (SSL) protocol in sessions with compatible clients. The use of SSL can provide server authentication, data integrity, and, optionally, client authentication and data encryption.

For this discussion, references to the SSL protocol should be considered applicable to the Transport Layer Security (TLS) protocol unless otherwise noted. Version 1 of the TLS protocol succeeded, but was not very different from, Version 3 of SSL.

Four general areas of consideration are discussed in this section:

- SSL Connection Options: For OS/390 Release 2.10 systems, a SECUREPORT port can be configured to allow basic, SSL, and negotiated SSL connections over the same port.
- Authentication: Server authentication is assumed in SSL, but client authentication is optional. In addition, various levels of client authentication can be selected.
- Certificate Management: Server certificates, Certificate Authority (CA) certificates, and, optionally, user certificates have to be managed.
- Encryption: Different strengths or no encryption are configuration options.

3.11.4.1 SSL CONNECTION OPTIONS

Some SSL connection options can have an important impact to security. The first of these applies to systems at OS/390 Release 2.10 and is associated with the use of the TELNETPARMS CONNTYPE and BEGINVTAM PARMSGROUP statements to alter the behavior of SECUREPORT ports. The second option controls a timeout value that applies during SSL connections.

Systems at OS/390 Release 2.10 can be configured to allow a SECUREPORT port to support different types of connections. The TELNETPARMS CONNTYPE statement has the following options:

SECURE: SECURE is the default value and matches the behavior of earlier OS/390 releases. It specifies that an SSL or negotiated SSL connection is permitted.

NEGTSECURE: NEGTSECURE specifies that a negotiated SSL connection is permitted.

BASIC: BASIC specifies that a basic (i.e., non-SSL) connection is permitted.

ANY: ANY specifies that a basic, SSL, or negotiated SSL connection is permitted.

NONE: NONE specifies that no connection is permitted. This is used together with a BEGINVTAM PARMSGROUP statement that overrides this setting with different CONNTYPE values for specifically identified clients.

While sites may select any appropriate CONNTYPE configuration, the following guidelines apply:

- Special care should be taken in choosing the BASIC or ANY options. Using one of these options allows a session to be connected on a SECUREPORT port and to use non-SSL processing. Such a session would not use the authentication or encryption features offered by SSL.
- Sites should maintain at least one port defined with a CONNTYPE of SECURE. This ensures that there is a port on which SSL processing is always performed.
- A TELNETPARMS SSLTIMEOUT statement defines the SSL handshake timeout value. For connections eligible for SSL processing, the Telnet server initiates the SSL handshake process and waits for a response from the client. If there is no response within the number of seconds specified by the SSLTIMEOUT statement, the server tries any additional connection types permitted by the TELNETPARMS configuration. If an SSL connection is required and the client does not respond in time, the connection is closed. A large number of connections, waiting for an extended period, could create a denial of service condition.
- Sites should choose an SSLTIMEOUT value that accommodates network performance without allowing individual connections to wait for an extended period. An SSLTIMEOUT value between 5 (the default) and 300 should be used.

3.11.4.1 AUTHENTICATION

Authentication is one of the primary features of SSL processing. The identity of the server and optionally the client is authenticated through the use of digital certificates. The Telnet Server supports server only or server and client authentication.

Server authentication is performed for all SSL connections. It is the process in which the client authenticates the server using the certificate provided by the server during connection processing. The required statements are TELNETPARMS SECUREPORT and, for OS/390 Release 2.10, TELNETGLOBALS KEYRING. These statements define the IP port used for the connection and the location of the digital certificates. Please refer to Section 4.4.2.1.1, PROFILE.TCPIP Configuration Statements, for the required settings.

Client authentication is optional for SSL connections. It is the process in which the server authenticates the client using the certificate provided by the client during connection processing. In addition to the statements necessary for server authentication, a TELNETPARMS CLIENTAUTH statement is required. Options on the CLIENTAUTH statement, along with resources defined in the SAF SERVAUTH class, can be used to configure three levels of client authentication.

- The first level of client authentication is specified by the SSLCERT operand on a TELNETPARMS CLIENTAUTH statement. It provides the lowest level of client authentication. In this level the server validates the certificate sent from the client and checks to verify that the Certificate Authority that signed the client's certificate is considered trusted by the server. Please refer to the following section on certificate management for a discussion on the issue of Certificate Authorities.

- The second level of client authentication is specified by the SAFCERT operand on a TELNETPARMS CLIENTAUTH statement. This level adds an additional check to the first level. In the second level, client certificates should be registered in advance with the ACP. This registration provides a map from a certificate to an ID defined to the ACP. During connection processing, after the level 1 check, a lookup of the client's certificate in the ACP's database is performed. If the ACP does not have an ID associated with the certificate, the connection is not permitted. It should be noted that it is possible to use a facility known as certificate name filtering. Under this facility, individual user certificates are not defined to the ACP. Instead, criteria are defined to the ACP that allows multiple certificates to be mapped to a single ID, based on selected fields from the certificate. Please refer to the following section on certificate management for a discussion on the issue of certificate name filtering.

- The third level of client authentication is specified by a combination of the SAFCERT operand on a TELNETPARMS CLIENTAUTH statement and the definition of resources in the SERVAUTH SAF class. This level adds an additional check to the first two levels. In the third level, the ID that has been assigned by the ACP should have access to the appropriate resource in the SERVAUTH SAF class. This resource represents the specific IP port provided by the specific TCP/IP address space on the system. It has the form EZB.TN3270.sysname.tcpipname.PORTnnnnn, where sysname refers to the value of the MVS SYSNAME system symbol that is defined in SYS1.PARMLIB(IEASYMxx), tcpipname identifies the TCP/IP address space, and PORTnnnnn identifies the port number. During connection processing, after the Level 1 and 2 checks, a check is made to determine that the assigned ID has access to the resource that represents the IP port. If the ACP determines that the access is not allowed, the connection is not permitted.

The DISA STIG provides the following guidelines for controls and the responsibilities of individuals within the organization.

- As resources permit, client authentication should be used for as many users as possible. Level 1 authentication is less desirable; Level 2 or 3 authentication should be used.

- For users that hold special privileges within the ACP, Level 2 or 3 authentication should be used whenever possible.

3.11.4.1 CERTIFICATE MANAGEMENT

Digital certificates are a primary requirement for SSL processing. In this section the following considerations in managing certificates are discussed:

- Location: There are multiple options for storing certificates that the Telnet Server can access.
- Origin: The origin of a certificate, the Certificate Authority, is crucial in determining if the certificate should be trusted.
- Name filtering: Multiple certificates can be mapped to a single ID.
- On OS/390 systems, an MVS data set, an HFS file, or, for OS/390 Release 2.10 and above, the resident ACP can be the storage location for digital certificates used by the Telnet Server. When certificates are stored in MVS data sets or HFS files, the GSKKYMAN utility is used to manipulate them. When they are stored by the ACP, commands specific to the ACP are used.

The DISA STIG offers the following guidance for storing Digital certificates:

- On OS/390 systems at Release 2.10 and above, the ACP should be used as the location for certificates. On older systems, an MVS data set should be used.
- Each digital certificate includes Certificate Authority (CA) information as the logical origin of the certificate. The presence of the CA's information indicates, to some level of trust, that the owner of the certificate is recognized by that CA to be who they claim to be. Each host maintains a list of CAs that are considered trusted. When client authentication is utilized, the CA from the client's certificate is compared to the host's list. If there is a match, a major criterion of SSL authentication is satisfied. Therefore, the list of CAs maintained on the host has a crucial impact on authentication decisions.
- Software is available on most host platforms, including OS/390, which allows a host to act as a Certificate Authority. When certificates are created on that host for use on that host, the certificates are considered to be self-signed. Certificates that are self-signed are generally considered to be of limited security value because no independent oversight of user identification is maintained.

Certificate name filtering is a facility that allows multiple certificates to be mapped to a single ACP ID. Rather than matching a certificate stored in the ACP to look up an ID, certificate name filtering uses criteria rules stored in the ACP. A filter rule uses parts of the distinguished name of the certificate owner and/or issuer (CA) to determine an ID to assign to the user. Depending on the filter criteria, a large number of client certificates could map to a single ID.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. Responsibilities delegated to the IAO should be performed by an authorized and knowledgeable individual. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that for production environments, the list of Certificate Authorities considered trusted by the OS/390 host are limited to those with a trust hierarchy that leads to a DOD PKI Root Certificate Authority.
- The IAO will ensure that for production environments, self-signed certificates are not used.

- The IAO will ensure that certificate name filtering is not used unless the filtering rules have been documented to, and approved by, the IAM.

3.11.4.2 ENCRYPTION

A key benefit from using SSL is the data privacy that is provided by session encryption. During the SSL connection process a mutually acceptable encryption algorithm is selected by the server and client. This algorithm is used to encrypt the data that subsequently flows between the two. However, the level or strength of encryption can vary greatly. In fact, certain configuration options can allow no encryption to be used; others can allow a relatively weak 40-bit algorithm to be used.

A TELNETPARMS ENCRYPTION statement is used to specify the encryption algorithms that the Telnet Server can use on the associated port.

The DISA STIG provides the following techniques for controls and the responsibilities of individuals within the organization. Responsibilities delegated to the IAO should be performed by an authorized and knowledgeable individual. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that a TELNETPARMS ENCRYPTION statement is coded for each statement block that defines a SECUREPORT.
- The systems programmer responsible for supporting ICS will ensure that to prevent the use of null or 40-bit encryption, each TELNETPARMS ENCRYPTION statement does not specify any of the following operands—SSL_NULL_Null, SSL_NULL_MD5, SSL_NULL_SHA, SSL_RC4_MD5_EX, or SSL_RC2_MD5_EX.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.4 SSL Connections.

3.11.5 SMF RECORDING

As determined by the TELNETPARMS SMFINIT and SMFTERM statements, the Telnet Server can provide audit data in the form of SMF records. SMF record type 118, the TCP/IP Statistics record, can be written with the following subtypes:

20 – Session initiation

21 – Session termination

SMF data produced by the Telnet Server provides information about individual sessions. The data includes the VTAM application, the remote and local IP addresses, and the remote and local IP port numbers. This data may provide valuable information for security audit activities.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The systems programmer responsible for supporting ICS will ensure that the TELNETPARMS SMFINIT and SMFTERM statements are coded with the STD operand within each TELNETPARMS statement block.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 4.4.2.1.5 SMF Recording.

3.12 MONITORING CONTROLS

All mainframe system activity is logged by an MVS component called the System Management Facilities (SMF). A properly configured SMF provides a large amount of data on system activity and performance that can be analyzed for decision-making, and thereby to manage the system. This data is also used to produce activity, violation and other security reports.

3.12.1 SYSTEM AUDITING FEATURES - SMF DATA COLLECTION

SMF collects data from all manner of sub-processes and formats it into pre-defined record types. Some of the types of data SMF records are regarding:

- System configuration
- Paging activity
- Workload
- CPU time and performance
- SYSOUT activity
- Dataset activity
- Security-related events
- Attempts to gain access to unauthorized resources

Mainframe support departments can decide what kinds of system events should be included in the system log (SMF) data. Each type of SMF data has a corresponding numeric value between 0-256 called a record type. Records generated by a core set of SMF record types should be recorded at all times, however there are more types that should be enabled depending on the client's needs and mainframe operating environment. Enabling record types does come at a cost however. As more record types are captured in SMF data, more overhead is placed on the system to capture and write these events to disk and more disk space is required to store the resulting data.

The STIG requires the audit trail to record the identity of the user, time of access, interaction with the system, and sensitive functions that might permit a user or program to modify, bypass, or negate security safeguards. SMF data presents a critical component in providing the required audit trails to maintain OS/390 system integrity. All relevant SMF data will be collected and retained for at least one year to ensure that adequate audit trails are available.

Settings to control the collection of SMF data are found in SYS1.PARMLIB member SMFPRMxx. The STIG recommends the following settings should be configured for optimal collection of SMF data:

Table 5 SMF Parameters and Settings

SMF Parameters and Settings	
ACTIVE	Activates the collection of SMF data.
JWT(15)	The maximum amount of consecutive time that an executing job may spend as ineligible to use any CPU resources before being cancelled for inactivity. The STIG requirement for Job Wait Time is 15 minutes. (This may be extended if controlled through other means, e.g., a Session Manager or ACP.)
MAXDORM(0500)	Specifies the amount of real-time that SMF allows data to remain in an SMF buffer before it is written to a recording data set.
SID	Specifies the system ID to be recorded in all SMF records.
SYS(DETAIL)	Controls the level of detail recorded.
SYS(INTERVAL)	Ensures the periodic recording of data for long-running jobs.
SYS	Specifies the types and sub-types of SMF records that are to be collected. SYS(TYPE) indicates that the supplied list is inclusive (i.e., specifies the record types to be collected). Record types not listed are not collected. SYS(NOTYPE) indicates that the supplied list is exclusive (i.e., specifies those record types not to be collected). Record types not listed are not collected. The site may use either form of this parameter to specify SMF record type collection. However, at a minimum all record types listed in the SMF Data Collection table above will be collected.

Thousands of log entries, or messages, are written to SMF throughout a normal day of mainframe processing. As these messages are generated, they are written to pre-allocated SMF buffers and datasets. An SMF buffer is a defined area of memory that collects SMF data. Because of the frequency of SMF data, it is inefficient to write data to relatively slow disk storage and instead is queued in memory.

Once the SMF buffer in memory fills its space allocation, the data is written out to a dataset using the IBM supplied IFASMFDP program. The SMF datasets are typically named SYS1.MANx; the number of datasets depends on the volume log SMF data generated. Like the SMF buffer, the MANx datasets have a predetermined size and may fill its space allocation. When this happens, the system will begin writing to the next available SMF dataset. If no empty SMF dataset is found, SMF can be configured to either halt the entire MVS system or continue operations but drop any additional SMF log data.

Due to the volume and format of data collected, raw SMF data is not immediately useful to system administrators or other end users. SMF report generating software, either developed internally or purchased from companies such as Vanguard or SAS, processes SMF data on a regular basis to produce reports used by managers to make system management decisions and monitor system violations logged by SMF. During the creation of these reports, data may be temporarily stored in user-specified datasets on the system.

Since the SYS1.MANx datasets are holding activity log data, access to them should be restricted. Furthermore, if SMF data is selected from these datasets and used in subsequent processes (e.g. backed up to tape, used in report writing routines), access to the data should be protected at each step along the way to preserve the integrity of log data.

The DISA STIG provides the following recommendation to ensure control over SMF Data Collection; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The SMFPRMxx member will specify, at a minimum, all record types noted in the SMF Data Collection table above. SMF data collection will be activated. Specify a unique system ID for each domain to ensure that SMF data can be discretely identified to, and associated with, the domain where it originated.

2) All update and alter access authority to SMF files (MANx) will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the SMF files (MANx). The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

3) To ensure that all SMF data is collected in a timely manner, and to reduce the risk of data loss, the site will ensure that automated mechanisms are in place to collect and retain all SMF data produced on the system. Dump the SMF files (MANx) in DOD systems based on the following guidelines:

   a) Dump each SMF file as it fills up during the normal course of daily processing.

   b) Dump all remaining SMF data at the end of each processing day.

4) In OS/390 systems, SMF data is the ultimate record of system activity. Therefore, SMF data is of the most sensitive and critical nature. While the length of time for which SMF data will be retained is not specifically regulated, it is imperative that the information is available for the longest possible time period in case of subsequent investigations. The statute of limitations varies according to the nature of a crime. It may vary by jurisdiction, and some crimes are not subject to a statute of limitations. Apply the following guidelines to the retention of SMF data for all DOD systems:

   a) Retain at least two (2) copies of the SMF data.

   b) Maintain SMF data for a minimum of one year.

   c) All update and alter access authority to SMF history files will be logged using the ACP's facilities. Only systems programming personnel and batch jobs that perform SMF functions will be authorized to update the SMF files. The IAO will maintain the access requirements, and will maintain and review the ACP logging reports.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that collection options for SMF Data are consistent with options specified in this STIG.

- The IAO will ensure that update and allocate access to SMF collection files (i.e.SYS1.MANx) is limited to system programmers and/or batch jobs that perform SMF

dump processing, unless a letter justifying access is filed with the IAO, and all dataset access is logged.

- The IAO will ensure that an automated process is in place to collect SMF data.
- The IAO will ensure that update and allocate access to datasets used to backup and/or dump SMF collection files is limited to system programmers and/or batch jobs that perform SMF dump processing, unless a letter justifying access is filed with the IAO, and all dataset access is logged.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.10 SMF Data Collection.

3.12.1 AUDIT LOGS

The review of audit logs is an essential function of comprehensive security. Audit logs document vital information about system usage, including attempts to login to the system, access datasets, or use system resources. By reviewing these logs, managers can identify attempts to gain unauthorized access to the system and other usage trends which require investigation.

On the MVS operating system, the System Management Facility (SMF) captures a record system activity. Refer to System Auditing Features – SMF Data Collection above for an explanation of SMF and SMF record types. Records collected by SMF are used by report writing software to produce the security reports for review by support staff. While each ACP provides a default set of reports for the monitoring of system access activity, sites may choose to develop custom reports or reporting solutions specific to the site's needs.

Reviews of audit logs should be conducted on a daily, weekly, monthly, and quarterly basis, depending on the nature of activity being reviewed. Following are the DISA STIG requirements concerning the review of audit logs/security reports.

On a daily basis, the following audit entries will be reviewed:

- Data Set Access Violations: Sensitive data sets (i.e., APF authorized libraries, ACP libraries, LPA libraries, LINKLIST libraries, etc.) are the top priority. Look for patterns of denied access. Does the same user or group of users keep showing up in the log?
- Resource Violations: This is a varied category that includes items such as transactions (e.g., CICS, DB2, IDMS, CA1, etc.), to job classes, to operator commands, etc.
- Program Use Violations: Applies primarily to Sensitive Utilities (refer to Section 3.1.5.3, Sensitive Utility Controls). Attempts to use these by unauthorized users and jobs need to be questioned.

On a weekly/monthly basis (more often if time permits), the following audit entries will be reviewed:

- Failed Logon Attempts: Password miss-types are common. The reviewer should be looking for excessive violations for a single user or a block of users such as a department.

- Special Privileges: Changes to logonids where special privileges or attributes (e.g., SECURITY for ACF2, ACCESS[ALL] for TOP SECRET, SPECIAL for RACF) were given need to be reviewed for legitimacy.

On a quarterly basis, the following audit entries will be reviewed:

- The accesses from TRUSTED STCs to ensure there is no abuse occurring.
- FTP userids/logonids/ACIDs to ensure their accesses are appropriate.

In addition, in regards to Global Control Options the DISA STIG states that any changes need to be evaluated to ensure they were authorized and legitimate.

The DISA STIG provides the following technique for controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that the ACP audit logs are reviewed as specified above in the STIG.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, 2.1.4.3 Audit Logs.

4 CONCLUSION

This document is meant to relay pertinent information within the STIG to CMS and applicable CMS contractors. This document does not cover all topics discussed in the DISA STIG and is not intended to be used as a substitute to the STIG. In addition, access privileges denoted within this document and DISA STIG may not be suitable for every organization, meaning that each organization may choose to be more restrictive. Because every organization is unique not all aspects of this document or the DISA STIG may be applicable.

This document is to be used as a guide to securing organization environments, and by following the recommendations and techniques within organizations will be able to secure the confidentiality and integrity of their data and resources.

Appendix A – CMS Minimum Security Requirements (CMSRs)

Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, Appendix A, *CMS Minimum Security Requirements for High Impact Level Data*, for the applicable CMSRs.

Appendix B - Glossary and Acronym Listing

ACEE	Access Control Environment Element
ACF2	Access Control Facility 2
ACID	Accessor ID
ACPs	Access Control Products
APF	Authorized Program Facility
BLP	Bypass Label Processing
CA	Computer Associates or Certificate Authority
CAISSF	CA's International Standard Security Facility
CDT	Class Descriptors Table
CICS	Customer Information Control System
CMP	Change Management Process
CMS	Centers for Medicare and Medicaid Services
CMSRs	CMS Minimum Security Requirements
CPU	Central Processing Unit
CWF	Common Working File
DAA	Designated Approval Authority
DAT	Dynamic Access Translation
DCA	Departmental Control Acid
DD	Data Definition
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information System Agency
DMERCs	Durable Medical Equipment Regional Carriers
DoD	Department of Defense
EDC	Enterprise Data Centers
ETMS	External Tape Management System
FI	Fiscal Intermediary
FTP	File Transfer Protocol
FTPD	File Transfer Protocol daemon program

FTPDNS	File Transfer Protocol server program
GSO	Global Systems Options
HFS	Hierarchical File System
HHS	Health and Human Services
HLQ	High Level Qualifier
IAC	Installation Account Code
IANA	Internet Assigned Numbers Authority
IAO	Information Assurance Officer
IBM	International Business Machines
ICS	Internet Connection Sharing
IMS	Information Management System
IP	Internet Protocol
IPL	Initial Program Load
ISPF	Interactive System Productivity Facility
IT	Information Technology
I/O	Input/Output
JCL	Job Control Language
JWT	Job Wait Time
LAN	Local Area Network
LID	Logonid
LSCA	Limit Control ACID
LU	Logical Unit
MAC	Medicare Administrative Contractors
MCS	Multiple Console Support
MSCA	Master Security Control ACID
MUSASS	Multi User Single Address Space System
MVS	Multi-Processing Virtual Storage or Multiple Virtual System
NCP	Network Control Program
OIG	Office of the Inspector General
O/S	Operating System

PADS	Program Access to Data Sets
PPGM	Protected Program List
PPT	Program Properties Tables
PROC	JCL procedure
RACF	Resource Access Control Facility
SAF	System Authorization Facility
SCA	Security Control ACID
SDLC	Synchronous Data Link Control
SDSF	System Display and Search Facility
SID	SMF System ID
SMF	System Management Facilities
SNA	System Network Architecture
SPECLU	Specified Logical Unit
SSL	Secure Sockets Layer
STC	Started Task Control
STIG	Security Technical Implementation Guide
SVC	Supervisor Calls
TLS	Transport Layer Security
TSO	Time Sharing Option
TSS	TOP SECRET
USS	Unformatted System Services
VCA	Divisional Control ACID
VTAM	Virtual Telecommunication Access Method
ZCA	Zone Control ACID

Appendix C - Default Values for Sample Program Properties Table (PPT)

APPENDIX B. SAMPLE PROGRAM PROPERTIES TABLE (PPT)

The following table depicts the default values for the Program Properties Table (PPT), as provided by IBM in module **IEFSDPPT** for OS/390, Version 2 Release 10. Please refer to the IBM *OS/390 MVS Initialization and Tuning Reference* documentation for the version and release of OS/390 installed at the individual site for the actual contents of the default **IEFSDPPT** module.

PROGRAM NAME	*PROGRAM DESCRIPTION*	*NC*	*NS*	*PR*	*ST*	*ND*	*BP*	*KEY*	*PROC AFFINITY*	*2P*	*1P*	*NP*
AHLGTF	GTF	X	X		X			00	NONE			X
AKPCSIEP	ISP		X		X	X		01	NONE			X
ANFFIEP	IP Printway		X		X	X		01	NONE			
APSPPIEP	PSF		X		X	X		01	NONE			X
ASBSCHIN	APPC/MVS Scheduler Address Space (ASCH)		X		X			01	NONE	X	X	
ASBSCHWL	APPC/MVS Message Log Writer			X				01	NONE			
ATBINITM	APPC/MVS Address Space		X		X			01	NONE	X	X	
ATBSDFMU	APPC/MVS SDFM Utility			X				01	NONE			
AVFMNBLD	AVM	X	X		X			03	NONE			X
BPXINIT	OMVS	X	X		X			00	NONE			
BPXPINPR	OMVS	X			X			08	NONE	X	X	
BPXVCLNY	OMVS		X	X	X			08	NONE			
CBRIIAS	OTIS				X			05	NONE			
CBROAM	OAM		X		X			05	NONE			
CNLSSDT	MVS Message Service (MMS)		X		X			00	NONE	X	X	
COFMINIT	VLF		X		X	X	X	00	NONE			
COFMISDO	DLF	X	X		X	X	X	00	NONE			
CQSINIT0	IMS CQS		X		X			07	NONE			X
CSVLLCRE	LLA		X		X		X	00	NONE			
CSVVFRCE	Virtual Fetch		X		X			00	NONE			
DFSMVRC0	IMS Control Program		X		X			07	NONE			
DSNUTILB	DB2 Batch							07	NONE			

This table was taken directly from the DISA OS/390 & z/OS STIG Appendix B.

PROGRAM NAME	PROGRAM DESCRIPTION	NC	NS	PR	ST	ND	BP	KEY	PROC AFFINITY	2P	1P	NP
DSNYASCP	DB2		X		X			07	NONE			
DXRRLM00	IMS Manager		X		X			07	NONE			
EPWINIT	FFST	X	X			X	X	00				X
ERBMFMFC	RMF		X		X	X		08	NONE			
ERB3GMFC	RMF		X		X	X		08	NONE			
EZAPPAAA	NPF		X					08				
EZAPPFS	NPF		X					01				
EZBTCPIP	TCP/IP Address Space	X	X	X	X			06		X	X	
GDEICASB	DFP/DFM		X		X			05	NONE			X
GDEISASB	DFP/DFM				X			05	NONE			X
GDEISBOT	DFP/DFM		X		X			05	NONE			X
HASJES20	JES2	X	X		X	X		01	NONE			
HHLGTF	GTF	X	X		X			00	NONE			X
IASXWR00	External Writer	X			X			01	NONE			
IATCNDTK	JES3	X	X	X	X			01	NONE			
IATINTK	JES3	X	X		X	X		01	NONE			
IATINTKF	JES3 FSS		X		X	X		01	NONE			
IDAVSJST	SMSVSAM Address Space	X	X	X	X			05	NONE			
IEAVTDSV	Dumping Services			X	X		X	00	NONE	X	X	
IEDQTCAM	TCAM		X					06	NONE			X
IEEMB860	Master	X	X		X	X	X	00	NONE			
IEEVMNT2	Mount Command	X			X			00	NONE			
IEFIIC	Initiator	X		X	X			00	NONE			
IFASMF	SMF	X	X	X	X	X		00	NONE			
IFDOLT	OLTEP							08	NONE	X	X	
IGDSSI01	SMS	X	X		X		X	05	NONE			
IGG0CLX0	CAS	X	X	X	X	X		00	NONE	X		
IHLGTF	GTF	X	X		X			00	NONE			X
IKTCAS00	TCAS	X		X	X			06	NONE			

This table was taken directly from the DISA OS/390 & z/OS STIG Appendix B.

PROGRAM NAME	*PROGRAM DESCRIPTION*	*NC*	*NS*	*PR*	*ST*	*ND*	*BP*	*KEY*	*PROC AFFINITY*	*2P*	*1P*	*NP*
IOSVROUT	IOS	X	X		X		X	00	NONE			
IRRSSM00	RACF	X	X	X	X			02	NONE			
ISFHCTL	SDSF		X					01	NONE			
ISTINM01	VTAM	X	X		X		X	06	NONE			X
ITTTRCWR	CTRACE Writer Address Space	X	X	X	X		X	00	NONE	X	X	
IWMINJST	WLM	X	X		X			00	NONE			X
IXCINJST	XCF	X	X		X			00	NONE	X	X	
IXGBLF00	System Logger Address Space		X		X			00	NONE			
IXGBLF01	System Logger Address Space	X	X		X			00	NONE	X	X	
IXZIX00	JES Common Coupling Address Space	X	X	X	X			01	NONE			
MVPTNF	TNF Address Space	X	X	X	X			00	NONE			
MVPXVMCF	VMCF Address Space	X	X	X	X			00	NONE			
SNALINK	SNALINK Address Space		X		X			06	NONE			

This table was taken directly from the DISA OS/390 & z/OS STIG Appendix B

References

- IBM International Technical Support Information. (May, 1996). P*lanning for a CA-ACF2 Migration to OS/390 Security Sever (RACF)* Redbook.
- OS/390-Z/OS Security. (2004). *Audit and Control Features*. Peter Thingsted
- IBM Poughkeepsie Services Center. (September, 1999). *Security Server (RACF) Introduction.*
- IBM International Technical Support Information. (October, 2002). *Communications Server for z/OS V1R2 TCP/IP Implementation Guide Volume 2: UNIX Applications* Redbook.
- The Henderson Group. (February, 2006). *How to Audit MVS, RACF, ACF2, CICS, and DB2 Security.*
- IBM. (April 2006). I*ntroduction to New Mainframe: Networking*. Mike Ebbers, Wayne O'Brien, Bill Ogden.
- IBM (July 2006). *Introduction to New Mainframe: z/OS Basics.* Mike Ebbers, Chris Hastings.
- http://www.sdsusa.com/dictionary/
- http://www-03.ibm.com/systems/z/
- http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp

(This Page Intentionally Blank)