



Using Vanguard Security Solutions to Complete DISA STIG SRR Review Procedures

z/OS RACF Analysis Process and Checklist

Modeled After:
SRR REVIEW PROCEDURES
z/OS RACF Checklist
Developed by Vanguard Integrity Professionals
Version 6 Release 43

February 06, 2020

Using Vanguard Security Solutions™ to Complete DISA STIG SRR Review Procedures

DISA Version 6.39

Document Number RACF_STIG-08012016-084600-628A

January 2019

Copyright

© 1989-2014 Vanguard Integrity Professionals-Nevada.

All rights reserved. Printed in the USA.

No part of this publication may be copied, reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, for any purpose other than the Licensee's personal use, without express written permission from Vanguard Integrity Professionals-Nevada.

Trademarks

Vanguard Integrity Professionals, Vanguard Administrator, Vanguard Advisor, Vanguard Analyzer, Vanguard Authenticator, Vanguard Cleanup, Vanguard Configuration Manager, Vanguard Enforcer, Vanguard ez/AccessControl, Vanguard ez/SignOn, Vanguard ez/SignOn Deploy, Vanguard ez/Integrator, Vanguard ez/Token, Vanguard GRC, Vanguard IAM, Vanguard Identity Manager, Vanguard Identity & Access Management, Vanguard Governance, Risk Management and Compliance, Vanguard inCompliance, Vanguard Offline, Vanguard OPID Manager, Vanguard PasswordReset, Vanguard Policy Manager, Vanguard Registration Manager, Vanguard SecurityCenter, Vanguard Security Conference, Vanguard Security on Demand, Vanguard Security Solutions, Vanguard Security Suite, AutoPilot, eDistribution, Enterprise-Wise, Vanguard Deploy, Vanguard ez/Security on Demand, Find-it-Fix-it-Fast, Knowledge Expo, Pathway to Profitability, QS/390, QuickGen, Quality Security Framework, Quality Security/390 Suite, Registration Manager, RioVision, RiskMinder, Security on Demand, SmartAssist, SmartLink, SmartPanel, and Vanguard Tokenless Authentication are trademarks or service marks of Vanguard Integrity Professionals-Nevada.

AIX, AS/400, IBM logo and the Business Partner emblem, CICS, DB2, IMS, MVS/ESA, OS/400, RACF, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other products mentioned in this publication, including Linux, Red Hat, SUSE, UNIX, Solaris and HP-UX, are trademarks or registered trademarks of their respective owners.

About This Product

Any software products accompanying this publication are copyrighted and owned by Vanguard Integrity Professionals-Nevada. Use of the software product is governed by the provisions of your License Agreement or the Terms of Use on the envelope in which the software product was sent to you. **Warranty and Limitation of Liability:** VANGUARD warrants that the licensed software products as delivered do not infringe any patent or copyright held by any third party and enforceable under U.S. law. THE FOREGOING WARRANTY IS THE SOLE AND EXCLUSIVE WARRANTY PROVIDED BY VANGUARD UNDER OR IN CONNECTION WITH THE LICENSED SOFTWARE PRODUCTS AND IS IN LIEU OF ALL OTHER WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NONINFRINGEMENT. UNDER NO CIRCUMSTANCES WILL VANGUARD BE LIABLE TO CUSTOMER FOR ANY OF THE FOLLOWING: (I) ANY DAMAGES CAUSED BY THE FAILURE OF CUSTOMER TO PERFORM ITS RESPONSIBILITIES; (II) ANY THIRD-PARTY

CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES; OR (III) ANY LOST PROFITS, LOSS OF BUSINESS, LOST SAVINGS OR OTHER CONSEQUENTIAL, SPECIAL, INCIDENTAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, EVEN IF INFORMED OF THEIR POSSIBILITY.

Table of Contents

z/OS Data Analysis.....	15
___STIG ID: AAMV0010.....	15
___STIG ID: AAMV0012.....	17
___STIG ID: AAMV0014.....	18
___STIG ID: AAMV0018.....	19
___STIG ID: AAMV0030.....	20
___STIG ID: AAMV0040.....	21
___STIG ID: AAMV0050.....	22
___STIG ID: AAMV0060.....	23
___STIG ID: AAMV0160.....	24
___STIG ID: AAMV0325.....	25
___STIG ID: AAMV0350.....	26
___STIG ID: AAMV0370.....	27
___STIG ID: AAMV0380.....	29
___STIG ID: AAMV0400.....	31
___STIG ID: AAMV0410.....	32
___STIG ID: AAMV0420.....	33
___STIG ID: AAMV0430.....	34
___STIG ID: AAMV0440.....	35
___STIG ID: AAMV0450.....	36
___STIG ID: AAMV0500.....	38
RACF Data Analysis.....	41
___STIG ID: ACP00010.....	41
___STIG ID: ACP00020.....	42
___STIG ID: ACP00030.....	43
___STIG ID: ACP00040.....	44
___STIG ID: ACP00050.....	45
___STIG ID: ACP00060.....	46
___STIG ID: ACP00062.....	48
___STIG ID: ACP00070.....	49
___STIG ID: ACP00080.....	51
___STIG ID: ACP00100.....	52
___STIG ID: ACP00110.....	54
___STIG ID: ACP00120.....	56
___STIG ID: ACP00130.....	57
___STIG ID: ACP00135.....	58
___STIG ID: ACP00140.....	59
___STIG ID: ACP00150.....	60
___STIG ID: ACP00170.....	61
___STIG ID: ACP00180.....	62
___STIG ID: ACP00190.....	63
___STIG ID: ACP00200.....	64
___STIG ID: ACP00210.....	65

___ STIG ID: ACP00220.....	66
___ STIG ID: ACP00230.....	67
___ STIG ID: ACP00240.....	68
___ STIG ID: ACP00250.....	69
___ STIG ID: ACP00260.....	70
___ STIG ID: ACP00270.....	72
___ STIG ID: ACP00282.....	74
___ STIG ID: ACP00291.....	76
___ STIG ID: ACP00292.....	77
___ STIG ID: ACP00293.....	80
___ STIG ID: ACP00294.....	82
___ STIG ID: ACP00320.....	84
___ STIG ID: ACP00330.....	86
___ STIG ID: ACP00340.....	87
___ STIG ID: ACP00350.....	89
___ STIG ID: RACF0244.....	90
___ STIG ID: RACF0246.....	91
___ STIG ID: RACF0248.....	92
___ STIG ID: RACF0250.....	93
___ STIG ID: RACF0260.....	94
___ STIG ID: RACF0280.....	96
___ STIG ID: RACF0290.....	97
___ STIG ID: RACF0300.....	98
___ STIG ID: RACF0310.....	99
___ STIG ID: RACF0320.....	101
___ STIG ID: RACF0330.....	102
___ STIG ID: RACF0350.....	103
___ STIG ID: RACF0360.....	104
___ STIG ID: RACF0370.....	105
___ STIG ID: RACF0380.....	106
___ STIG ID: RACF0400.....	107
___ STIG ID: RACF0420.....	108
___ STIG ID: RACF0430.....	109
___ STIG ID: RACF0440.....	110
___ STIG ID: RACF0445.....	111
___ STIG ID: RACF0450.....	112
___ STIG ID: RACF0460.....	113
___ STIG ID: RACF0462.....	114
___ STIG ID: RACF0465.....	116
___ STIG ID: RACF0467.....	117
___ STIG ID: RACF0470.....	118
___ STIG ID: RACF0480.....	119
___ STIG ID: RACF0490.....	120
___ STIG ID: RACF0500.....	121
___ STIG ID: RACF0510.....	122
___ STIG ID: RACF0520.....	123

__STIG ID: RACF0540.....	124
__STIG ID: RACF0550.....	125
__STIG ID: RACF0560.....	126
__STIG ID: RACF0570.....	127
__STIG ID: RACF0580.....	128
__STIG ID: RACF0590.....	129
__STIG ID: RACF0595.....	131
__STIG ID: RACF0600.....	132
__STIG ID: RACF0620.....	134
__STIG ID: RACF0650.....	135
__STIG ID: RACF0660.....	139
__STIG ID: RACF0680.....	141
__STIG ID: RACF0690.....	143
__STIG ID: RACF0710.....	145
__STIG ID: RACF0720.....	146
__STIG ID: RACF0730.....	148
__STIG ID: RACF0740.....	149
__STIG ID: RACF0760.....	150
__STIG ID: RACF0770.....	151
__STIG ID: RACF0780.....	152
Digital Certificates Data Analysis	153
__STIG ID: ICERR010.....	153
__STIG ID: ICERR020.....	154
__STIG ID: ICERR030.....	155
CICS Data Analysis	157
__STIG ID: ZCIC0010	160
__STIG ID: ZCIC0020	162
__STIG ID: ZCICR021.....	164
__STIG ID: ZCIC0030	165
__STIG ID: ZCIC0040	169
__STIG ID: ZCIC0041	171
__STIG ID: ZCICR041.....	173
__STIG ID: ZCIC0042	174
FEP Data Analysis	176
__STIG ID: ZFEP0011	176
__STIG ID: ZFEP0012	177
__STIG ID: ZFEP0013	178
__STIG ID: ZFEP0014.....	179
__STIG ID: ZFEP0015	180
__STIG ID: ZFEP0016.....	181
IBM Communications Server Data Analysis.....	182
__STIG ID: IFTP0010.....	182
__STIG ID: IFTP0020	183
__STIG ID: IFTP0030	185
__STIG ID: IFTP0040	187
__STIG ID: IFTP0050	188

___STIG ID: IFTP0060	190
___STIG ID: IFTP0070	191
___STIG ID: IFTP0080	193
___STIG ID: IFTP0090	195
___STIG ID: IFTP0100	196
___STIG ID: IFTP0110	197
___STIG ID: ISLG0010	199
___STIG ID: ISLG0020	200
___STIG ID: ISLG0030	201
___STIG ID: ITCP0010	203
___STIG ID: ITCP0020	204
___STIG ID: ITCP0025	205
___STIG ID: ITCP0030	206
___STIG ID: ITCP0040	208
___STIG ID: ITCP0050	210
___STIG ID: ITCP0060	212
___STIG ID: ITCP0070	213
___STIG ID: ITCPR052	215
___STIG ID: ITNT0020	219
___STIG ID: ITNT0030	221
___STIG ID: ITNT0050	223
___STIG ID: ITNT0060	225
___STIG ID: IUTN0010	226
___STIG ID: IUTN0020	227
___STIG ID: IUTN0030	228
___STIG ID: IUTN0040	230
JES2 Data Analysis	231
___STIG ID: ZJES0011	231
___STIG ID: ZJES0014	233
___STIG ID: ZJES0021	234
___STIG ID: ZJES0022	237
___STIG ID: ZJES0031	238
___STIG ID: ZJES0032	242
___STIG ID: ZJES0041	244
___STIG ID: ZJES0042	245
___STIG ID: ZJES0044	247
___STIG ID: ZJES0046	249
___STIG ID: ZJES0052	252
___STIG ID: ZJES0060	254
DFSMS Data Analysis	256
___STIG ID: ZSMSR008	256
___STIG ID: ZSMS0010	257
___STIG ID: ZSMS0012	260
___STIG ID: ZSMS0020	261
___STIG ID: ZSMS0022	263
___STIG ID: ZSMS0030	264

__STIG ID: ZSMS0032	265
TSO Data Analysis	266
__STIG ID: ZTSO0020	266
__STIG ID: ZTSO0030	267
UNIX System Services Data Analysis.....	268
__STIG ID: ZSSH0010.....	268
__STIG ID: ZSSH0020.....	269
__STIG ID: ZSSH0030.....	270
__STIG ID: ZSSH0040.....	272
__STIG ID: ZSSH0050.....	273
__STIG ID: ZUSS0011.....	274
__STIG ID: ZUSS0012.....	275
__STIG ID: ZUSS0013.....	276
__STIG ID: ZUSS0014.....	277
__STIG ID: ZUSS0015.....	278
__STIG ID: ZUSS0016.....	279
__STIG ID: ZUSS0021.....	281
__STIG ID: ZUSS0022.....	282
__STIG ID: ZUSS0023.....	283
__STIG ID: ZUSS0031.....	284
__STIG ID: ZUSS0032.....	285
__STIG ID: ZUSS0033.....	286
__STIG ID: ZUSS0034.....	287
__STIG ID: ZUSS0035.....	288
__STIG ID: ZUSS0036.....	289
__STIG ID: ZUSS0041.....	290
__STIG ID: ZUSS0042.....	291
__STIG ID: ZUSS0043.....	292
__STIG ID: ZUSS0044.....	293
__STIG ID: ZUSS0045.....	294
__STIG ID: ZUSS0046.....	295
__STIG ID: ZUSS0047.....	296
__STIG ID: ZUSS0048.....	297
__STIG ID: ZUSS0080.....	298
__STIG ID: ZUSSR050.....	302
__STIG ID: ZUSSR060.....	303
__STIG ID: ZUSSR070.....	304
VTAM Data Analysis	305
__STIG ID: ZVTM0011	305
__STIG ID: ZVTM0018	306
WebSphere Applications Server Data Analysis	307
__STIG ID: ZWAS0010	307
__STIG ID: ZWAS0020	308
__STIG ID: ZWAS0030	311
__STIG ID: ZWAS0040	312
__STIG ID: ZWAS0050	313

MQSeries/WebSphere MQ Data Analysis.....	314
___STIG ID: ZWMQ0011.....	314
___STIG ID: ZWMQ0012.....	316
___STIG ID: ZWMQ0014.....	318
___STIG ID: ZWMQ0020.....	320
___STIG ID: ZWMQ0030.....	321
___STIG ID: ZWMQ0040.....	323
___STIG ID: ZWMQ0049.....	326
___STIG ID: ZWMQ0051.....	328
___STIG ID: ZWMQ0052.....	330
___STIG ID: ZWMQ0053.....	331
___STIG ID: ZWMQ0055.....	336
___STIG ID: ZWMQ0056.....	338
___STIG ID: ZWMQ0057.....	340
___STIG ID: ZWMQ0058.....	341
___STIG ID: ZWMQ0059.....	342
___STIG ID: ZWMQ0060.....	344

Change Log:

01/09/2017 – Release of DISA 6.29. The following two checks were added:

- ACP00062
- RACF0540
- Updates were made to the DISA STIG ADDENDUM for ZMVZR020 and ZISFR020 but those did not affect the instructions in those documents.

8/1/2016 – Release of DISA 6.28. The following changes are part of this release:

- ZVSSR020
 - Added new resource VSR\$.SCOPE (see addendum for list of who is permitted access). READ access is permitted when approved/documented by ISSM or equivalent Security Authority.
- IBM SDSF Document
 - Document name changed from zOS IBM System Display and Search FACILITY (SDSF) for RACF to zOS IBM SDSF for RACF
- ICERR0010
 - New check added
- ICERR0020
 - New check added
- ICERR0030
 - New check added
- AAMV0016
 - Check has been deleted
- ITNT0040
 - Chec has been deleted
- ACP00270

Removed “If the products BMC Mainview, CA 1, and/or CA Common Services are on the system, the RACF access to the CSVDYLPA resource and/or generic equivalent will be defined with AUDIT(ALL) and UPDATE access restricted to BMC Mainview, CA 1, and CA Common Services STC users”. Replaced with “If any software product requires access to dynamic LPA updates on the system, the RACF access to the CSVDYLPA resource and/or generic equivalent will be defined with LOG and SERVICE(UPDATE) only after the product has been validated with the appropriate STIG or SRG for compliance AND receives documented and filed authorization that details the need and any accepted risks from the site ISSM or equivalent security authority”.

- ACP00282
 - Change to state “Access at the MVS.** level must not be granted”. This can be found in the STIG Addendum, Table 7-1: Controls on z/OS System Commands)
- ZUSS0048
 - Updated to cover all accounts used for modeling in creating UNIX accounts. This includes the OMVS default user and BPX.UNIQUE.USER
- ZSMS0010
 - Add resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE with access NONE and all access logged
- ZJES0060
 - Wording changed to restrict authorization to scheduling tools, started tasks, and other system applications required to run production jobs. Also added “Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent)”.
- ZSSH0010
 - New check added
- ZSSH0020
 - New check added
- ZSSH0030
 - New check added
- ZSSH0040
 - New check added
- ZSSH0050
 - New Check added

4/26/2016 – Release of DISA 6.27. The following changes are part of this release:

- ZISFR002
 - Add statement saying if the operating system is at release 2.2 or higher the check may not be applicable.
- ZTADR001
 - Add READ access to job scheduling products and System Auditors.
- RACF0467
 - New check added.

1/28/2016 – Release of DISA 6.26. The following changes are part of this release:

- ACP00270
 - Add CSVLYLPA.ADD.**. The CSVLYLPA.ADD resource will be permitted to products BMC Mainview, CA 1, and CA Common Services STC userids with AUDIT(ALL(READ)) and UPDATE access.
 - Add CSVLYLPA.ADD.**. The CSVLYLPA.DELETE resource will be permitted to products CA 1 and CA Common Services STC userids with AUDIT(ALL(READ)) and UPDATE access.
- RACF0465 – New check added.

10/30/2015 – Changes to 6.25

- ZAIDR001 Remove UPDATE access for domain level security administrators.
- ZAIDR002 New check added.
- ZCTRR002 Add READ access to BMC Users.
- ZIOAR001 Add UPDATE access to BMC Administrators. Add READ access to BMC Users.
- Addendum Updates
 - Table 11-3: BMC Control-M Resources – Added Resource \$\$JOBORD.qname.userid. READ access allowed for Application batch production userids (APPBAUDT).
 - Table 11-36: BMC MAINVIEW Resources – Added access to System Programmers (SYSPAUDT) for resources BBM.PLEXMGR.targetid.MYB30.OD and BBM.PLEXMGR.targetid.MYD00.OD.

07/29/2015 – Changes to 6.24

- ZCTOR001 Updated to allow OPERAUDT READ access to the BMC CONTROL-O STC Datasets.
- Removed the following STIGs:
 - ZDBM0010
 - ZIDM0010
 - ZIDM0014
 - ZIDM0020
 - ZIDM0030
 - ZIDM0032
- ZJES0032 Updated to specify “The RACF resources and/or generic equivalent in the WRITER class are defined with a default access of NONE. The RACF resource access authorizations are defined with UACC(NONE) and NOWARNING”. Updated to include “If the Classification of the system is unclassified, this is not applicable”.
- ZMIMR020 Updated to allow AUTOAUDT UPDATE access to resource MIMGR.FREE.
- ZWMQ0014 STIG added back in (was removed in 6.23).
- Removed Addendum Sections 11.10; IDMS Requirements and 11.17, Supported Software.

05/21/2015 – Change to 6.23

- Changed ZCTRR002 adding alter access to Production Control and Scheduling Personnel and Automated Operations.
- Changed ZCLSR042 CAC logon processing exit from KLVSFPTX to KLSNFPTX.
- Changed ZISFR020. Removed Operations (OPERAUDT) and System Programmers (SYSPAUDT) access to GROUP.group-name.server-name with group-name containing AUPDT greater than 0. Will require additional analysis to justify access. Updated z/OS STIG Addendum.
- Changed ZISF0040. Added requirement for AUPDT=0. All GROUP statements that specify a value greater than 0 for AUPDT will require justification for the setting.
- Changed ACP00120 adding requirement that the dataset that contains the REXX for Password exit must be included in the files to be protected.
- Changed RACF0460 to say at least **one** RULE needs to be at least 8 chars long. RACF0460 makes no mention what the other RULEs must be which means the other RULEs can be anything. In prior releases the restrictions are on every RULE defined.
- Added RACF0462.
- Removed ZWMQ0014.
- Addendum updates:
 - Table 11-37: BMC MAINVIEW Resources
 - Added Resource BBM.PLEXMGR.targetid.MYB30.OD with access given to User Group MV STCs
 - Added Resource BBM.PLEXMGR.targetid.MYD00.OD with access given to User Group MV STCs
 - Table 11-43: Parameters for RACF IRRPWREX
 - Table added to support addition of DISA STIG RACF0462 which has been added with this release.

04/22/2015 - Added Control Correlation Identifier (CCI) numbers to all STIGs

10/2014 - Changed ZNET0040 removing SECOPTS.OPERSEC=SAFPW as an additional configuration option.

Changed Product scripts for Telnet to recognize multiple entries for SMFINIT and SMFTERM in TelnetGlobals and TelnetParms blocks.

Changed z/OS Addendum

- Added paragraph 11.1 “General Installed Product Information” explaining the use of dataset examples.
- Added paragraph 5.1.3 “Password Complexity” which adds new RESERVED WORD/PREFIX LIST.
- Updated CICS Transaction security categories.
- Amended access for certain CICS management transaction to include application programmers in the CICS list

08/25/2014 change to 6.20

Modified the list of SMF records in AAMV0380

Added READ access for Auditors and DASD BATCH jobs in ACP00120

Changed audit requirements in ACP00120

Modified ACP00270: Modified to the following:

2. On the Access List report, if access to all CSV-prefixed resources is restricted to only systems personnel, there is NO FINDING.

(In addition:

- Access to resource CSVLLA can include CICS userids and Control-O userids (if Control-O is installed on your system) in addition to systems programmers and there is NO FINDING
- READ access to resource CSVDYNEX.LIST is permitted to auditor userids and there is NO FINDING
- If the products BMC Mainview, CA 1, and/or CA Common Services are on the system, the RACF access to the CSVDYLPA resource and/or generic equivalent will be defined with AUDIT(ALL) and UPDATE access restricted to BMC Mainview, CA 1, and CA Common Services STC userids.

Note: In the above, UPDATE access can be substituted with ALTER or CONTROL. Review the permissions in the IBM documentation when specifying UPDATE

Added following note to RACF0580

Note: FTP only process and server to server userids may have PASSWORD(NOINTERVAL) specified. These users must be identified in the FTPUSERS group in the Dialog Process or FTP in the name field. Additionally these users must change their passwords on an annual basis.

05/2014 – change to 6.19

Added AAMV0012, AAMV0016, ACP00210, and ZCIC0010.

Changed:

RACF0270 – Removed DATASET, GROUP, and USER, since classes are always active.

RACF0580 - Removed requirement for TSO PROC

ZWMQ0011 – Added additional cipher specifications

02/2014 – added changes to 6.18

Changed CAT 2 to CAT 1, ACP00030, ACP00040, ACP00050, ACP00070, ACP00080, ACP00100, ACP00120, ACP00130, ACP00170, ACP00240, ZDBM0010, ZTSO0020, ZUSS0022, and ZUSS0023.

Changed IFTP0060 and ITNT0060 evaluation to allow TYPE119.

Changed ITNT0040 to identify additional DoD Approved External PKIs.

ZCIC0010 Removed.

AAMV0012 Removed.

AAMV0016 Removed.

ZSRRR000 Added domain level production control and scheduling personnel to the types of users.

04/2012 – Change log moved to STIG Instruction Manual

3/29/2012 Modified ACP00260, ACP00350, IFTP0110, ADDED RACF0445
Removed SDSF, CA_1, NC_PASS STIGS from this document and put into three separate documents.

8/11/2011 Added ZUSS0080, Modified ITNT0040, RACF0360 , ZCA10035 and ZJES0060 for V6.8 compatibility.

5/11/2011 Modified RACF0360, RACF0620, ZJES0044, ZWMQ0054 and ZWMQ0059 for Version 6.7 Stig compatibility

11/25/2010 Modified ZSMS0010, removed All ZIOA Checks.
Modified ITCP0050, ZCA10045.

09/22/2010 Modified RACF0260

09/22/2010 Modified RACF0510

10/06/2010 Added note to ZISF0340

10/06/2010 Added clarification to AAMV0450

10/08/2010 corrected ZUSS0013

10/08/2010 corrected ZJES0060

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

z/OS Data Analysis

___STIG ID: AAMV0010

Default Severity: Category III

- a) Generate a list of SMP/E CSI data sets using ISPF 3.4
 - 1. From ISPF 3.4 enter Dsname Level...*.*.CSI
- b) Execute the following sample JCL to generate a listing of installed products and features

```
//STEP1 EXEC PGM=GIMSMP,REGION=0M
//SYSPRINT DD SYSOUT=*
//SMPOUT DD SYSOUT=*
//SMPCSI DD DISP=SHR,DSN= << CSI DATA SET
//SMPLIST DD DSN=YOURHLQ.FEATURE.LIST,
//          DCB=(RECFM=FBA,LRECL=121,BLKSIZE=12100),
//          SPACE=(CYL,(1,1)),
//          DISP=(NEW,CATLG)
//SMPCNTL DD *
          SET BDY(GLOBAL) /* SET TO GLOBAL ZONE. */.
          LIST FEATURE.
/*
/*-----*
/* ADD STEPS AS REQUIRED FOR ALL ADDITIONAL CSI DATA SETS
/* REPORTS WILL BE APPENDED TO THE FEATURE LIST
/*+---1---+---2---+---3---+---4---+---5---+---6---+---7*
//STEP2 EXEC PGM=GIMSMP
//SYSPRINT DD SYSOUT=*
//SMPOUT DD SYSOUT=*
//SMPCSI DD DISP=SHR,DSN=ANOTHER.GLOBAL.CSI << ADDITIONAL CSI
//SMPLIST DD DSN=YOURHLQ.FEATURE.LIST,
//          DISP=MOD
//SMPCNTL DD *
          SET BDY(GLOBAL) /* SET TO GLOBAL ZONE. */.
          LIST FEATURE.
/*
```

NOTE 1: SMP/E CSIs may not be present on this domain. If the site uses another domain to install products via SMP/E, and then copies the SMP/E product installation libraries to this domain, this is acceptable.

Review the domain where the SMP/E environment resides and compare it against the domain being reviewed for compliance.

The **Z/OS STIG** states that all products with the capability for installation via IBM's SMP/E process will be installed and maintained using that process.

- c) If the entries contained in the SMP/E CSIs accurately reflect the operating system software environment, there is **NO FINDING**.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

- d) If the entries contained in the SMP/E CSIs do not accurately reflect the operating system software environment, this is a FINDING.

CCI: CCI-000326

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___STIG ID: AAMV0012

Default Severity: Category I

- a) Refer to the list of supported software products in the U_ZOS_STIG_Addendum.
- b) If the software products currently running on the reviewed system are at a version greater than or equal to the products listed in Appendix A then this is not a finding.
- c) If the software products currently running on the reviewed system are at a version less than the products listed in the z/OS STIG Addendum or additional products are APF authorized or access sensitive data, than this is a FINDING.

CCI: CCI-001764

CCI: CCI-001765

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___ **STIG ID: AAMV0014**

Default Severity: Category II

- a) Check with the Systems programmer to make sure that documented procedures exist to monitor the software products in checklist Appendix A to verify dates it will become unsupported and to notify management to start procedures to upgrade to supported versions of the products before that date.
- b) If documented procedures exist to monitor products in Appendix A for dates they will become unsupported and to notify management to upgrade to supported versions of the products this is not a finding.
- c) If documented procedures do not exist to monitor products in Appendix A for dates they will become unsupported and to notify management to upgrade to supported versions of the products this is a finding.

***Note:** If product support is provided through an outside group, verify that they have a process to notify site of unsupported software.*

CCI: CCI-000409

CCI: CCI-001225

CCI: CCI-001227

CCI: CCI-002606

CCI: CCI-002615

CCI: CCI-002617

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___ **STIG ID: AAMV0018**

Default Severity: Category I

- a) Check with the Information Assurance Officer to make sure that documented procedures exist for security related software patches to be scheduled, applied and documented.
- b) If the documented procedures exist to monitor, apply and document software patches than this is not a finding.
- c) If the documented procedures do not exist to monitor, apply and document software patches than this is a finding.

CCI: CCI-001220

CCI: CCI-002605

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___ **STIG ID: AAMV0030**

Default Severity: Category II

- a) From Analyzer main Menu, go to 3;L;<ENTER>
- b) Place a B next to the first occurrence of IEASYSnn
- c) If LNKAUTH=APFTAB is specified, there is NO FINDING.
- d) If LNKAUTH=APFTAB is NOT specified, this is a FINDING.

CCI: CCI-000381

CCI: CCI-001762

CCI: CCI-002283

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0040**

Default Severity: Category III

- a) From Analyzer main Menu, go to 4;B. Specify “S” next to APF table in the upper half of the screen. Specify “YES” for Exceptions Only and “NO” for all other options on the lower half of the screen. Submit the batch job and reference the report output.
- b) If there are no entries in the report with finding messages, there is NO FINDING for inaccessible APF Libraries.
- c) If there are no entries in the report with finding messages, there is NO FINDING for inaccessible APF Libraries.

CCI: CCI-000381

CCI: CCI-001762

CCI: CCI-002283

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___STIG ID: AAMV0050

Default Severity: Category III

- a) Refer to the list of Sensitive Utility Requirements in the U_ZOS_STIG_Addendum.
- b) From Analyzer main Menu, go to 4;B. Specify “S” next to APF tables in the upper half of the screen. Specify “YES” for Duplicate Module Analysis and “NO” for all other options on the lower half of the screen. Submit the batch job and reference the report output. Review the Duplicate Module Analysis section of the report.
- c) If duplicate APF modules exist, compare the duplicates to the modules specified in the U_ZOS_STIG_Addendum Sensitive Utility Requirements.
- d) If none of the sensitive utilities are duplicated, there is NO FINDING.
- e) If any of the sensitive utilities are duplicated, this is a FINDING.

CCI: CCI-001762

CCI: CCI-002283

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0060**

Default Severity: Category III

- a) Verify that there is annual review of all AC=1 modules in the APF libraries.
- b) Verify that there is documentation of the justification for these modules to be in the APF libraries.
- c) Verify that there is documentation proving the integrity of the modules in the APF libraries such as source code etc.
- d) For vendor-supplied modules the documentation can be in the form of Product Installation Guides and Product Systems Programming Guides.
- e) If all of the above is true there is NO FINDING
- f) If any of the above is not true there is a FINDING.

CCI: CCI-000643

CCI: CCI-001829

CCI: CCI-002736

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0160**

Default Severity: Category II

- a) From Analyzer main Menu, go to 4;A. Specify “YES” for Perform Module Search, “YES” for Exceptions Only, and “NO” for Sort Criteria. Submit the batch job and reference the report output.
- b) Review report for any entries with message “VSA334R”.
 1. If any of the entries in the report that have message “VSA334R” associated with them have any of the following settings, then there is a **FINDING**:
 - a. Bypass password protection: Yes
 - b. No Dataset Integrity? Yes
 - c. Protect Key (if required): 00-07
 2. If **ALL** of the entries in the report that have message “VSA334R” associated with them **DO NOT** have any of the following settings, then there is **NO FINDING**:
 - a. Bypass password protection: Yes
 - b. No Dataset Integrity? Yes
 - c. Protect Key (if required): 00-07

CCI: CCI-000381

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0325**

Default Severity: Category III

- a) From Analyzer main Menu, go to 4;B. Specify “S” next to LPA List table in the upper half of the screen. Specify “YES” for Exceptions Only and “NO” for all other options on the lower half of the screen. Submit the batch job and reference the report output.
- b) If there are no entries in the report with finding messages, there is NO FINDING for inaccessible LPA List Libraries.
- c) If there are entries in the report with finding messages, there is a FINDING for inaccessible LPA List libraries.

CCI: CCI-001762

CCI: CCI-001764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0350**

Default Severity: Category III

- a) From Analyzer main Menu, go to 4;B. Specify “S” next to Link List Table (All libraries) in the upper half of the screen. Specify “YES” for Exceptions Only and “NO” for all other options on the lower half of the screen. Submit the batch job and reference the report output.
- b) If there are no entries in the report with finding messages, there is NO FINDING for inaccessible LINKLIST Libraries.
- c) If there are entries in the report with finding messages, there is a FINDING for inaccessible LINKLIST libraries.

CCI: CCI-001762

CCI: CCI-001764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0370**

Default Severity: Category II

- a) From Analyzer main Menu, go to 3;L;<ENTER>
- b) Place a B next to the first occurrence of SMFPRMnn
- c) If all the options for SMF data gathering are set as required (in the table shown at the end of this STIG) there is NO FINDING.

NOTE: Issues with subtype 4 and 5 of type 30 records can be exempted from collection. The following is an example of the entry to perform this:

**SUBSYS(STC,EXITS(IEFU29,IEFU83,IEFU84,IEFUJP,IEFUSO),
INTERVAL(SMF,SYNC),NODETAIL)**

NOTE: If the JWT parameter is greater than 15 minutes, and the system is processing unclassified information, review the following items. If any of these items is true, there is NO FINDING.

- d) If a session is not terminated, but instead is locked out after 15 minutes of Inactivity, a process must be in place that requires user identification and Authentication before the session is unlocked. Session lock-out will be Implemented through system controls or terminal screen protections.
- e) A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision.
- f) The IAM may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:

The time-out exception cannot exceed 60 minutes.

A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site IAM. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).

The requirement must be revalidated on an annual basis.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

If variances from the below SMF collection options (with the exception of the ones mentioned in (b) above), this is a FINDING.

The settings for several parameters are critical to the collection process:

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 canceled 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.

CCI: CCI-000057

CCI: CCI-000130

CCI: CCI-001844

CCI: CCI-001851

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0380**

Default Severity: Category II

- a) From Analyzer main Menu, go to 4;H. Specify “YES” next to Record Type cross-reference and “NO” for all other options. Submit the batch job and reference the report output. Review the Record Type Cross-reference section of the report.
- b) If all of the required SMF record types (as specified below in the table IBM SMF RECORDS TO BE COLLECTED AT A MINIMUM) are being collected, there is NO FINDING.
- c) If any of the required record types is not being collected, this is a FINDING.

IBM SMF RECORDS TO BE COLLECTED AT A MINIMUM

0 (00) –	IPL
6 (06) –	External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) –	[SMF] Data Lost
14 (0E) –	INPUT or RDBACK Data Set Activity
15 (0F) –	OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) –	Scratch Data Set Status
18 (12) –	Rename Non-VSAM Data Set Status
24 (18) –	JES2 Spool Offload
25 (19) –	JES3 Device Allocation
26 (1A) –	JES Job Purge
30 (1E) –	Common Address Space Work
32 (20) –	TSO/E User Work Accounting
41 (29) –	DIV Objects and VLF Statistics
42 (2A) –	DFSMS statistics and configuration
43 (2B) –	JES Start
45 (2D) –	JES Withdrawal/Stop
47 (2F) –	JES SIGNON/Start Line (BSC)/LOGON
48 (30) –	JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) –	JES Integrity
52 (34) –	JES2 LOGON/Start Line (SNA)
53 (35) –	JES2 LOGOFF/Stop Line (SNA)
54 (36) –	JES2 Integrity (SNA)
55 (37) –	JES2 Network SIGNON
56 (38) –	JES2 Network Integrity
57 (39) –	JES2 Network SYSOUT Transmission
58 (3A) –	JES2 Network SIGNOFF
60 (3C) –	VSAM Volume Data Set Updated
61 (3D) –	Integrated Catalog Facility Define Activity
62 (3E) –	VSAM Component or Cluster Opened

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

- 64 (40) – VSAM Component or Cluster Status
- 65 (41) – Integrated Catalog Facility Delete Activity
- 66 (42) – Integrated Catalog Facility Alter Activity
- 80 (50) – RACF/TOP SECRET Processing
- 81 (51) – RACF Initialization
- 83 (53) – RACF Audit Record For Data Sets
- 90 (5A) – System Status
- 92 (5C) except subtypes 10, 11 – OpenMVS File System Activity
- 102 (66) – DATABASE 2 Performance
- 103 (67) – IBM HTTP Server
- 110 (6E) – CICS/ESA Statistics
- 118 (76) – TCP/IP Statistics
- 119 (77) – TCP/IP Statistics
- 199 (C7) – TSOMON
- 230 (E6) – ACF2 or as specified in ACFFDR (vendor-supplied default is 230)
- 231 (E7) – TSS logs security events under this record type

CCI: CCI-000130

CCI: CCI-000131

CCI: CCI-000132

CCI: CCI-000133

CCI: CCI-000134

CCI: CCI-000135

CCI: CCI-000169

CCI: CCI-000172

CCI: CCI-001353

CCI: CCI-001487

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0400**

Default Severity: Category II

- a) Refer to Vulnerability Questions in the U_zOS_STIG_Addendum
 - 1. Ensure all documents are current and being followed.
- b) Ensure at least the following are covered in the documents.
 - 1. Retain at least two (2) copies of the SMF data
 - 2. Maintain SMF data for a minimum of one year
 - 3. 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.
- c) If, based on the information provided, it can be determined that an automated process is in place to collect and retain all SMF data produced on the system, and all items in section b are being adhered to, there is NO FINDING
- d) If it cannot be determined this process exists and is being adhered to, or that any one item in section b is not followed, this is a FINDING.

CCI: CCI-001348

CCI: CCI-001353

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0410**

Default Severity: Category II

- a) From Analyzer main Menu, go to 4;3. Specify “NO” for all options on the screen. Submit the batch job and reference the report output. Review the RACF Databases section of the report.
- b) If the RACF database is not located on the same volume as either its alternate or backup database, there is NO FINDING.
- c) If the RACF database is located on the same volume as either its alternate or backup database, there is a FINDING

CCI: CCI-000549

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0420**

Default Severity: Category II

Refer to the Vulnerability Questions in the U_z/OS STIG_Addendum

- a) If, based on the information provided, it can be determined that the RACF database is being backed up on a regularly scheduled basis, there is NO FINDING.
- b) If it cannot be determined that the RACF database is being backed up on a regularly scheduled basis, this is a FINDING.

CCI: CCI-000537

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0430**

Default Severity: Category II

Refer to Vulnerability Questions in the U_zOS_STIG_Addendum

- a) If, based on the information provided, it can be determined that system DASD backups are performed a regularly scheduled basis, there is NO FINDING.
- b) If it cannot be determined that system DASD backups are performed on a regularly scheduled basis, this is a FINDING.

CCI: CCI-000537

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___**STIG ID: AAMV0440**

Default Severity: Category II

- a) From Analyzer main Menu, go to 3;G. Record the SYSRES Volume serial number. From Administrator main Menu, go to 8;3. Enter “PASSWORD” in the Dsname Level field. Enter the SYSRES Volume serial number in the Volume serial field. <ENTER>.
- b) If the message “NO FILES MATCH DSN LVL” is returned, there is NO FINDING.
- c) If the PASSWORD dataset shows up on the report, this is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

STIG ID: AAMV0450

Default Severity: Category II

- a) From Analyzer main Menu, go to 4;B. Enter “S” next to APF tables. Enter “YES” next to AC(1) module list and NO to all other options in lower half of the screen. Submit the batch job. Refer to the report. Review any locally developed modules in the AC(1) list by APF authorized library per item (g) below.
- b) From Analyzer main Menu, go to 3;C. <ENTER>. Refer to online report. Ensure that any item with a YES under CMD, PGM or TSF is reviewed per item (g) below.
- c) From Analyzer main Menu, go to 4;E. Enter “NO” to all options on the screen. Submit the batch job. Refer to the report. If you see this in the report “There are 0 User I/O Appendages defined for use.” then no finding for I/O appendages. Otherwise, review the I/O appendages listed per item (g) below.
- d) From Analyzer main Menu, go to 4;J. Enter “NO” to all options on the screen. Submit the batch job. Refer to the report. Review all locally developed exits listed per item (g) below.
- e) From Analyzer main Menu, go to 4;A. Enter “NO” to all options on the screen. Submit the batch job. Refer to the report. Review all modules with SPEC KEY = YES, BYP PASS = YES or PROT KEY = 7 or less that was locally developed per item (g) below.
- f) From Analyzer main Menu, go to 4;D. Enter “S” next to all data sources. Enter “NO” to all options on the lower half of the screen. Submit the batch job. Refer to the report looking for any Locally Defined USER SVCs (Usually between 200 and 255) per item (g) below.
- g) Ensure the following items are in effect:
 - 1. The acquisition of any new IA and IA-enabled Commercial-Off-the-Shelf (COTS) products meets the applicable Common Criteria, NIAP, or FIPS evaluation and validation requirements specified in NSTISSP No. 11 and DODI 8500.2 or receives DAA approval.
 - 2. All locally developed extensions to the operating system environment (i.e., operating system exits, SVCs, I/O appendages, modules requiring special PPT privileges and APF authorization) have been reviewed by the site’s system programmer to assure that requirements of CNSSP No. 11 and DODD 8500.1 are met and/or approved by site DAA.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

h) If both items in (g) are true for all system programs, there is NO FINDING.

i) If any item in (g) is untrue for a system program, this is a FINDING.

CCI: CCI-000271

CCI: CCI-000633

CCI: CCI-000634

CCI: CCI-001806

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 41

___STIG ID: AAMV0500

Default Severity: Category II

- a) To get a list of all shared DASD:
 - From Analyzer main menu, select option 4;0 (DASD Analysis). This will generate a report of all DASD with a flag showing if it is shareable or not.
 - On the VOLUME ANALYSIS menu that is presented, enter 'YES' next to VTOC Analysis so that the list of datasets on each volume will be displayed.
- b) Check the VTOC list of datasets for any critical or sensitive datasets (such as APF, LINKLIST, LPA, Catalog or Product-type Data sets).
- c) The IAO and/or Systems programming personnel must review / verify that there is a justification for having these data sets on shared DASD and that there is justification for the systems that have access to the shared DASD to access the critical/sensitive datasets that may be on them.
- d) If (c) is true there is NO FINDING.
- e) If (c) is not true there is a FINDING.

CCI: CCI-000099

CCI: CCI-001090

CCI: CCI-001414

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

Set up for RACF Data Analysis multiple STIG reporting

1. Allocate a dataset or pds 80 bytes in length, fixed blocked; this dataset will be used to hold the dataset name(s) to be analyzed as required by the following STIGs.
2. Edit above dataset and input dataset name(s), when multiple dataset are being analyzed, enter one per line beginning in column 1.

The dataset names and associated STIGs are:

• SYS1.PARMLIB	ACP00010
• SYS1.LINKLIB	ACP00020
• SYS1.SVCLIB	ACP00030
• SYS1.IMAGELIB	ACP00040
• SYS1.LPALIB	ACP00050
• SYS1.NUCLEUS	ACP00080
• RACF Database Name(s)	ACP00120
• Master Catalog Name	ACP00130
• User Catalog Name(s)	ACP00135
• SMP/E CSI Name(s)	ACP00140
• JES2 System Dataset Name(s)	ACP00150
• SYS1.UADS	ACP00170
• SMF Dataset Name(s)	ACP00180
• SMF Dump/Backup Name(s)	ACP00190
• System Dump Dataset Name(s)	ACP00200
• DASD Backup File Name(s)	ACP00210
• SYS1.TRACE	ACP00220
• System Page Datasets	ACP00230
• System Exit Lib Name(s)	ACP00240
• JES2 Proc Lib Name(s)	ACP00250

3. Generate batch report JCL, as follows:.
4. From Analyzer main Menu, go to option 4
5. Press <ENTER>
6. Select option B - Sensitive/Critical Data Sets Analysis
7. Press <ENTER>
8. Select User defined List option by entering an S next to the prompt and fill in the dataset name information at the bottom of the option list

Fully qualified (without quotes) name of data set containing list:

====> your.own.dataset.name.from.setup

Or

Fully qualified (without quotes) name of data set containing list:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

====> **your.own.;pds.name.from.setup(member-name)**

9. At the bottom of the screen, select the following options as shown below:

Specify YES or NO to include the following:

AC(1) module list ====> **NO** **Duplicate Module Analysis** ====> **NO**

RACF detail ====> **YES** **Exceptions only** ====> **NO**

RACF Group detail ====> **YES**

Search criteria ====> **NO**

Sort criteria ====> **NO**

10. Press <ENTER>

11. Select QG on the next panel, when the QG edit screen is displayed enter the following beginning in column 2

LD DA('&DSNAME') VOLUME(&DSVOL)

LD DA('&DSNAME') GEN

12. Type ACCEPT at the Command line

13. Press <ENTER>

14. Select E on the JCL Submit Processing panel, when the generated JCL is displayed modify the following:

//VSSQGOUT DD DSN=&&TEMPQG,UNIT=SYSALLDA,

// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),SPACE=(CYL,(1,1))

15. Add the following statements after the last generated JCL statement:

//STEP02 EXEC PGM=IKJEFT01

//SYSTSPRT DD SYSOUT=*

//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

RACF Data Analysis

___STIG ID: ACP00010

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.PARMLIB,
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule) with an access other than NONE, this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify, that
 - a. READ access is restricted to System Level Started Tasks, Authorized Data Center Personnel, Auditors, Systems Programmers and Domain Level Security Administrators, otherwise this is a finding.
 - b. UPATE access is only granted to Systems Programming Personnel and/or Domain Level Security Administrators
 - c. ALTER access is only been granted to System Programming Personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify, that
 - a. READ access is restricted to System Level Started Tasks, Authorized Data Center Personnel, Auditors, Systems Programmers and Domain Level Security Administrators, otherwise this is a finding.
 - b. UPATE access is only granted to Systems Programming Personnel and/or Domain Level Security Administrators
 - c. ALTER access is only been granted to System Programming Personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.PARMLIB and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a FINDING.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00020**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.LINKLIB,
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.LINKLIB and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00030**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.SVCLIB,
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.SVCLIB and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00040**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.IMAGELIB
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.IMAGELIB and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00050**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.LPALIB
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.LPALIB and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00060**

Default Severity: Category II

a) Generate batch report JCL, as follows:

1. From Analyzer main Menu, go to option 4
2. Press <ENTER>
3. Select option B - Sensitive/Critical Data Sets Analysis
4. Press <ENTER>
5. Select Authorized Program Facility (APF) Table by entering an S next to the prompt
6. At the bottom of the screen, select the following options as shown below:

Specify YES or NO to include the following:

AC(1) module list ===> NO Duplicate Module Analysis ===> NO
RACF detail ===> YES Exceptions only ===> NO
RACF Group detail ===> YES
Search criteria ===> NO
Sort criteria ===> NO

7. Press <ENTER>
8. Select QG on the next panel, when the QG edit screen is displayed enter the following beginning in column 2

LD DA('&DSNAME') VOLUME(&DSVOL)
LD DA('&DSNAME') GEN

9. Type ACCEPT at the Command line
10. Press <ENTER>
11. Select E on the JCL Submit Processing panel, when the generated JCL is displayed modify the following:

//VSSQGOUT DD DSN=&&TEMPQG, UNIT=SYSALLDA,
// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),
// SPACE=(CYL,(1,1))

b) Add the following statements after the last generated JCL statement:

//STEP02 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)

c) Review the report output for all listed libraries,

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a FINDING.
 2. Find the UACC field, if access is other than NONE, this is a FINDING
 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
- d) Review the RACF Dataset List output for all listed libraries and check Audit Flag settings
1. If UPDATE and/or ALTER failures and successes are not being logged this is a FINDING.
- e) If none of the above checks indicate a finding then there is NO FINDING.
- f) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00062**

Default Severity: Category I

- a) Refer to the following report produced by the Data Set and Resource Data Collection:

SENSITIVE.RPT(RACFREXX)

- b) Verify that the REXXLIB datasets are properly restricted. If the following guidance is true, this is NOT A FINDING.
- 1) RACF data set access authorizations restrict Update or higher access to z/OS systems programming personnel.
 - 2) RACF data set access authorizations restrict READ to Appropriate Started Tasks, Auditors, and the AXRUSER, specified in the PARMLIB AXR00 AXRUSER().
 - 3) All (i.e., failures and success) data set access authorities Update or Higher is logged
 - 4) RACF data set access authorizations specify UACC(NONE), that GAC is either NONE or not specified, and NOWARNING.
- c) If any of the above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00070**

Default Severity: Category I

- a) Generate batch report JCL, as follows:.
1. From Analyzer main Menu, go to option 4
 2. Press <ENTER>
 3. Select option B - Sensitive/Critical Data Sets Analysis
 4. Press <ENTER>
 5. Select LPA List Table by entering an S next to the prompt
 6. At the bottom of the screen, select the following options as shown below:

Specify YES or NO to include the following:

AC(1) module list ==> NO Duplicate Module Analysis ==> NO
RACF detail ==> YES Exceptions only ==> NO
RACF Group detail ==> YES
Search criteria ==> NO
Sort criteria ==> NO

7. Press <ENTER>
8. Select QG on the next panel, when the QG edit screen is displayed enter the following beginning in column 2

LD DA('&DSNAME') VOLUME(&DSVOL) ALL
LD DA('&DSNAME') GEN ALL

9. Type ACCEPT at the Command line
10. Press <ENTER>
11. Select E on the JCL Submit Processing panel, when the generated JCL is displayed modify the following:

//VSSQGOUT DD DSN=&&TEMPQG, UNIT=SYSALLDA,
// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),
// SPACE=(CYL,(1,1))

12. Add the following statements after the last generated JCL statement:

//STEP02 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- b) Review the report output for all listed libraries,
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a FINDING.
 - 2. Find the UACC field, if access is other than NONE, this is a FINDING.
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
- c) Review the RACF Dataset List output for all listed libraries and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- d) If none of the above checks indicate a finding then there is NO FINDING.
- e) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00080**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.NUCLEUS
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.NUCLEUS and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00100**

Default Severity: Category I

- a) Generate batch report JCL, as follows:
 1. From Analyzer main Menu, go to option 4
 2. Press <ENTER>
 3. Select option A - Program Properties Table Analysis
 4. Press <ENTER>
 5. At the bottom of the screen, select the following options as shown below:
"Perform module search" = Yes (sort doesn't matter)
EXCEPTION = No
 6. Press <ENTER>
 7. Select QG on the next panel, when the QG edit screen is displayed enter the following beginning in column 2
LD DA('&DSNAME') VOLUME(&DSVOL) ALL
LD DA('&DSNAME') GEN ALL
 8. Type ACCEPT at the Command line
 9. Press <ENTER>
 10. Select E on the JCL Submit Processing panel, when the generated JCL is displayed modify the following:
//VSSQGOUT DD DSN=&&TEMPQG, UNIT=SYSALLDA,
// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),
// SPACE=(CYL,(1,1))
- b) Add the following statements after the last generated JCL statement:
//STEP02 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)
- c) Review the report output for all listed libraries,
 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a FINDING.
 2. Find the UACC field, if access is other than NONE, this is a FINDING
 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
- d) Review the RACF Dataset List output for all listed libraries and check Audit Flag settings
 1. If UPDATE and/or ALTER failures and successes are not being logged this is a FINDING.
- e) If none of the above checks indicate a finding then there is NO FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

f) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00110**

Default Severity: Category II

- a) Generate batch report JCL, as follows:.
1. From Analyzer main Menu, go to option 4
 2. Press <ENTER>
 3. Select option B - Sensitive/Critical Data Sets Analysis
 4. Press <ENTER>
 5. Select Link List Table (All libraries) by entering an S next to the prompt
 6. At the bottom of the screen, select the following options as shown below:
Specify YES or NO to include the following:
AC(1) module list ===> NO Duplicate Module Analysis ===> NO
RACF detail ===> YES Exceptions only ===> NO
RACF Group detail ===> YES
Search criteria ===> NO
Sort criteria ===> NO
 7. Press <ENTER>
 8. Select QG on the next panel, when the QG edit screen is displayed enter the following beginning in column 2
LD DA('&DSNAME') VOLUME(&DSVOL) ALL
LD DA('&DSNAME') GEN ALL
 9. Type ACCEPT at the Command line
 10. Press <ENTER>
 11. Select E on the JCL Submit Processing panel, when the generated JCL is displayed modify the following:
//VSSQGOUT DD DSN=&&TEMPQG, UNIT=SYSALLDA,
// DISP=(,PASS),DCB=(RECFM=FB,LRECL=80),
// SPACE=(CYL,(1,1))
 12. Add the following statements after the last generated JCL statement:
//STEP02 EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD DSN=&&TEMPQG,DISP=(OLD,DELETE)
- b) Review the report output for all listed libraries,
1. Find the GAC field, if it shows a profile name (other than the Special Rule) with ACCESS other than NONE, this is a FINDING.
 2. Find the UACC field, if access is other than NONE, this is a FINDING.
 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a FINDING.
- c) Review the RACF Dataset List output for all listed libraries and check Audit Flag settings

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

1. If UPDATE and/or ALTER failures and successes are not being logged this is a FINDING.
- d) If none of the above checks indicate a finding then there is NO FINDING.
- e) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00120**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *RACF database Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), with ACCESS other than NONE, this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify READ access has only been granted to Auditors, DASD Batch jobs, system programming personnel, security personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify READ access has only been granted to Auditors, DASD Batch jobs, system programming personnel, security personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding
 - 5. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, security personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding.
 - 6. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, security personnel, and/or batch jobs that perform ACP maintenance, otherwise this is a finding.

NOTE: For RACF the dataset that contains the REXX for Password exit must be included in these files. Examine system REXLIB concatenation for this dataset name.

- b) Review the RACF Dataset List output for *RACF Database Name(s)* and check Audit Flag settings
 - 1. If All (i.e., failures and successes) data set access authorities (i.e. READ, UPDATE, ALTER, and CONTROL) for ACP security data sets and/or databases are not logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

CCI: CCI-002357

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00130**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *Master Catalog Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for *Master Catalog Name(s)* and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00135**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *User Catalog Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for *User Catalog Name(s)* and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00140**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *SMP/E CSI Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for *SMP/E CSI Name(s)* and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00150**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *JES2 System Dataset Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for *JES2 System Dataset Name(s)* and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00170**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.UADS
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE or lower access is restricted to Systems Programming Personnel and/or Security Personnel. Verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE or lower access is restricted to Systems Programming Personnel and/or Security Personnel. Verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for SYS1.UADS and check Audit Flag settings
 - 1. If ALL failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00180**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *SMF Dataset Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for *SMF Dataset Name(s)* and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00190**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *SMF Dump/Backup Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel and batch job userids that perform SMF processing, otherwise this is a finding.
 - 4. Under the Conditional Access list, verify UPDATE and ALTER access has only been granted to system programming personnel and batch job userids that perform SMF processing, otherwise this is a finding.
- b) Review the RACF Dataset List output for *SMF Dump/Backup Name(s)* and check Audit Flag settings. Verify that Audit Successes is set to READ or UPDATE, and Audit Failures is set to READ or UPDATE".
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000162

CCI: CCI-000163

CCI: CCI-000164

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00200**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *System Dump Dataset Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify READ, UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding. READ access has only been granted to personnel having justification to review the dump datasets for debugging purposes.
 - 4. Under the Conditional Access list, verify READ, UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding. READ access has only been granted to personnel having justification to review the dump datasets for debugging purposes.
- b) If none of the above checks indicate a finding then there is NO FINDING.
- c) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00210**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *DASD Backup File Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel and/or batch jobs that perform DASD backups, otherwise this is a finding.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00220**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: SYS1.TRACE
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify that READ or higher access has only been granted to system programming personnel and started tasks that perform GTF processing., otherwise this is a finding.
 - 4. Under the Conditional Access list, verify that READ or higher access has only been granted to system programming personnel and started tasks that perform GTF processing., otherwise this is a finding.
- b) If none of the above checks indicate a finding then there is NO FINDING.
- c) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00230**

Default Severity: Category II

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *System Page Dataset(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify READ or higher access has only been granted to system programming personnel, otherwise this is a finding.

- b) If none of the above checks indicate a finding then there is NO FINDING.

- c) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00240**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- a) Review the report output and locate Data set name: *System Exit Lib Name(s)*
 - 1. Find the GAC field, if it shows a profile name (other than the Special Rule), this is a finding.
 - 2. Find the UACC field, if access is other than NONE, this is a finding
 - 3. Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel, otherwise this is a finding.
- b) Review the RACF Dataset List output for *System Exit Lib Name(s)* and check Audit Flag settings
 - 1. If UPDATE and/or ALTER failures and successes are not being logged this is a finding.
- c) If none of the above checks indicate a finding then there is NO FINDING.
- d) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00250**

Default Severity: Category I

Note: Refer to Sensitive and Critical Dataset Report generated in Set up for RACF Data Analysis step at the beginning of this section.

- 1) Review the report output and locate Data set name: *JES2 Proc Lib Name(s)*
- 2) Find the GAC field, if it shows a profile name (other than the Special Rule), this is a FINDING.
- 3) Find the UACC field, if access is other than NONE, this is a FINDING.
- 4) Under the Standard Access list, verify UPDATE and ALTER access has only been granted to system programming personnel and READ access has only been granted to authorized users. If so, this is not a FINDING.
- 5) If none of the above checks indicate a finding then there is NO FINDING.
- 6) If any of the above checks indicate a finding then there is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00260**

Default Severity: Category II

Note: Generic profiles can be used (i.e. IEA*.** below instead of IEAABD*) for the checks below, as long as all the detailed requirements regarding access and logging as specified below, are met.

Memory and privileged program dump resources are provided via resources in the FACILITY resource class. Ensure that the following are properly specified in the ACP.

Display profiles for the IEAABD prefixed resources in the FACILITY resource class as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select General Resource Profile, option 4
- d) Press <ENTER>
- e) On the General Resource Reports screen, select Access List, option 4
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Profile field and enter IEAABD*
- h) Tab down to the Class field and enter FACILITY
- i) Press <ENTER>
- j) On the Processing Options panel, enter a Y next to 'Explode RACF groups in access list after detail line' prompt
- k) Press <ENTER>
- l) On the JCL Submit Processing screen, select S to submit the batch job
- m) Return to the General Reports screen, select Audit Flags, option 2
- n) Tab down to the Batch/Online field, type a B (for batch)
- o) Tab down to the Profile field and enter IEAABD*
- p) Tab down to the Class field and enter FACILITY
- q) Press <ENTER>
- r) On the JCL Submit Processing screen, select S to submit the batch job
- s) Review Access List report and Audit Flags report output and ensure that the following items are in effect:
 1. IEAABD.** is defined with a UACC(NONE) and AUDIT(ALL)
 2. IEAABD.DMPAUTH.** is defined with UACC(NONE) and SUCCESS(UPDATE) and FAILURES(UPDATE) or better specified. Only Systems Programmers are allowed UPDATE access. READ access is permitted to authorized users.
 3. IEAABD.DMPAKEY.** is defined with a UACC(NONE), AUDIT(ALL) and access is limited to Systems Programming Personnel only for any level of access.
- t) If any of the above in (s) is untrue for any of the specified IEAABD. resources, this is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00270**

Default Severity: Category II

Display profiles for the CSV-prefixed resources in the FACILITY resource class as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select General Resource Profile, option 4,
 - 1) Press <ENTER>
 - 2) On the General Resource Reports screen, select Access List, option 4
 - 3) Tab down to the Batch/Online field, type a B (for batch)
 - 4) Tab down to the Profile field and enter CSV*
 - 5) Tab down to the Class field and enter FACILITY
 - 6) Press <ENTER>
 - 7) On the Processing Options panel, enter a Y next to 'Explode RACF groups in access list after detail line' prompt
 - 8) Press <ENTER>
 - 9) On the JCL Submit Processing screen, select S to submit the batch job
 - 10) Return to the General Reports screen , select Audit Flags, option 2
 - 11) Tab down to the Batch/Online field, type a B (for batch)
 - 12) Tab down to the Profile field and enter CSV*
 - 13) Tab down to the Class field and enter FACILITY
 - 14) Press <ENTER>
 - 15) On the JCL Submit Processing screen, select S to submit the batch job
- d) Review Access List report and Audit Flags report output and ensure that the following items are in effect:
 - 1) On the Access List report, if the following resources are defined with a UACC (NONE), there is NO FINDING. On the Audit Flags report, if the following resources are defined with AUDIT(ALL), there is NO FINDING.

CSVAPF.**

CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC

CSVAPF.MVS.SETPROG.FORMAT.STATIC

CSVDYLPA.**

CSVDYLPA.ADD.**

CSVDYLPA.DELETE.**

CSVDYNEX.**

CSVDYNEX.LIST

CSVDYNL.**

CSVDYNL.UPDATE.LNKLST

(If CICS is installed on your system also include resource CSVLLA).

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- 2) On the Access List report, if access to all CSV-prefixed resources is restricted to only systems personnel, there is NO FINDING. In addition:
- Access to resource CSVLLA can include CICS userids and Control-O userids (if Control-O is installed on your system) in addition to systems programmers and there is NO FINDING
 - READ access to resource CSVDYNEX.LIST is permitted to auditor userids and there is NO FINDING
 - If any software product requires access to dynamic LPA updates on the system, the RACF access to the CSVDYLPA resource and/or generic equivalent will be defined with LOG and SERVICE(UPDATE) only after the product has been validated with the appropriate STIG or SRG for compliance AND receives documented and filed authorization that details the need and any accepted risks from the site ISSM or equivalent security authority.
 - If the products CA 1 and/or CA Common Services are on the system, the RACF access to the CSVDYLPA.DELETE resource and/or generic equivalent will be defined with AUDIT(ALL) and UPDATE access restricted to CA 1 and CA Common Services STC userids.
- Note:** In the above, UPDATE access can be substituted with ALTER or CONTROL. Review the permissions in the IBM documentation when specifying UPDATE
- 3) On the Audit Flags report, if access to all CSV-prefixed resources is logged, there is NO FINDING.
- 4) If any of the above is untrue for any CSV-prefixed resource, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00282**

Default Severity: Category II

Display System Commands Controls in the OPERCMDS class as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select General Resource Profile, option 4,
- d) Press <ENTER>
- e) On the General Resource Reports screen, select Access List, option 4
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Profile field and enter MVS*
- h) Tab down to the Class field and enter OPERCMDS
- i) Press <ENTER>
- j) On the Processing Options panel, enter a Y next to 'Explode RACF groups in access list after detail line' prompt
- k) Press <ENTER>
- l) On the JCL Submit Processing screen, select S to submit the batch job
- m) Return to the General Reports screen , select Audit Flags, option 2
- n) Tab down to the Batch/Online field, type a B (for batch)
- o) Tab down to the Profile field and enter MVS*
- p) Tab down to the Class field and enter OPERCMDS
- q) Press <ENTER>
- r) On the JCL Submit Processing screen, select S to submit the batch job
- s) Review Access List report and Audit Flags report output and ensure that the following items are in effect:

1. On the Access List report, if the MVS.** resource is defined to the OPERCMDS class with a default access of NONE, there is NO FINDING. On the Audit Flags report, if all failures and successes access to the MVS.** resource are logged, there is NO FINDING.

2. On the Access List report, if access to z/OS system commands defined in the table entitled *Controls on z/OS System Commands* in the **U_zOS_STIG_Addendum** is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), there is NO FINDING.

NOTE: Use the **GROUP** category specified in the table referenced above as a guideline to determine appropriate personnel access to system commands.

NOTE: The (MVS.SEND) Command will not be a finding if used by all.

3. In the STIG Addendum in the table entitled *Controls on z/OS System Commands* it is stated "Access at the MVS.** level must not be granted".

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

4. On the Audit Flag report, if all access (i.e., failures and successes) to specific z/OS system commands is logged as indicated in the table entitled *Controls on z/OS System Commands* in the **U_zOS_STIG_Addendum**, there is NO FINDING. Use the legend for Authorization meanings.

- t) If any of the above in (s) is untrue for any Z/OS system command resource, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00291**

Default Severity: Category II

Refer to the following items in SRR REVIEW PROCEDURES, Preliminary Worksheet (Part 1 of 2): Item 2

- a) Display PARMLIB information as follows:
 - 1. From Analyzer main Menu, go to option 3
 - 2. Press <ENTER>
 - 3. Select option L - Parmlib Analysis
 - 4. Press <ENTER>
 - 5. Press <ENTER> again
 - 6. On the next screen, look for entry CONSOLxx under the first LOADxx entry
 - 7. Enter V next to CONSOLxx to view details
 - 8. Press <ENTER>
 - 9. Either save the information to another dataset or print the dataset directly.

- b) Ensure the following items are in effect:
 - 1. The **CONSOLE** statement for each console specifies **AUTH(INFO)**.

***NOTE:** (a) The **AUTH** parameter is not valid for consoles defined with **UNIT(PRT)**. (b) Specifying **AUTH(MASTER)** is permissible for the system console.*

The **CONSOLE** statement for each console assigns a unique name using the **NAME** parameter.

- 2. The **DEFAULT** statement for each **CONSOLxx** member specifies **LOGON(REQUIRED)** or **LOGON(AUTO)**.
- c) If all of the above in (b) are true, there is NO FINDING.
- d) If any of the above in (b) is untrue, this is a FINDING.

CCI: CCI-000382

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00292**

Default Severity: Category II

Display CONSOLE userid information as follows:

- a) From Analyzer main Menu
 1. Go to option 3
 2. Press <ENTER>
 3. Select option L - Parmlib Analysis
 4. Press <ENTER>
 5. Press <ENTER> again
 6. On the next screen, look for entry CONSOLxx under the first LOADxx entry
 7. Enter V next to CONSOLxx to view details
 8. Press <ENTER>
 9. Either save the information to another dataset or print the dataset directly.
 10. Locate all console definitions by searching for NAME and noting each defined console name.

- b) In Administrator
 1. Select option 3 on the main menu
 2. Press <ENTER>
 3. Select User, option 1
 4. Press <ENTER>
 5. Select User Summary report, option 1
 6. Select the Batch option by changing the Batch/Online option to a B
 7. Select the Enhanced Masking option, enter Y
 8. On the Enhanced Masking panel, enter the following string:

userid = console1 or userid = console2 or userid = console3.....
 9. Press <ENTER>
 10. Select S on the JCL Submit Processing
 11. Press <ENTER>
 12. Review report output and ensure the following items are in effect:
 - a. Each console defined in the **CONSOLxx** parmlib members is associated with a valid RACF userid.
 - b. Ensure that RACF console userids are defined as follows:
 1. No special attributes (e.g., SPECIAL, OPERATIONS, etc.). If this is true there is NO FINDING.
 2. The RACF default group is the appropriate console group profile. If this is true, there is NO FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- c) In Administrator
1. Select option 3 on the main menu
 2. Press <ENTER>
 3. Select ID In Access List, option 17
 4. Press <ENTER>
 5. Enter U for ID Type and Console Userid for the ID field
 6. Select the Batch option by changing the Batch/Online option to a B
 7. Leave the Masking Fields of Profile and Class with an * in them. All profiles and classes will need to be searched for access.
 8. Set the UACC and * flags to Y, at the bottom of the screen
 9. Press <ENTER>
 10. Review report output and ensure the following item is in effect:
 - a. Restricted from accessing **all** data sets and resources except **MCS.MCSOPER.consolename** in the **OPERCMDS** resource class and **consolename** in the **CONSOLE** resource class. If this is true, there is NO FINDING.

Note: Repeat steps (5) thru (10) for each console userid.

- d) In Administrator
1. Select option 3 on the main menu
 2. Press <ENTER>
 3. Select User, option 1
 4. Press <ENTER>
 5. Select User Summary report, option 1
 6. Select the Enhanced Masking option, enter Y
 7. On the Enhanced Masking panel, enter the following string:

Userid = console1 or Userid = console2 or Userid = console3.....
 8. Press <ENTER>
 9. Enter the BRB line command next to the first userid listed on the report and on the last userid listed on the report
 10. Press <ENTER>
 11. Save command output to a dataset or PDS for future reference; review generated RACF commands and ensure console userids have no accesses to interactive on-line facilities (e.g., TSO, CICS, etc); if this is true, there is NOFINDING
- e) If all of the above in (b.12), (c.10) and (d.11) are true, there is NO FINDING.
- f) If any of the above in (b.12), (c.10) and (d.11) are not true, this is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

CCI: CCI-000382

CCI: CCI-002232

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00293**

Default Severity: Category II

Display CONSOLE class information as follows:

- a) From Analyzer main Menu
 1. Go to option 3
 2. Press <ENTER>
 3. Select option L - Parmlib Analysis
 4. Press <ENTER>
 5. Press <ENTER> again
 6. On the next screen, look for entry CONSOLxx under the first LOADxx entry
 7. Enter V next to CONSOLxx to view details
 8. Press <ENTER>
 9. Either save the information to another dataset or print the dataset directly.
 10. Locate all console definitions by searching for NAME and noting each defined console name.
- b) In Administrator
 1. Select option 3 on the main menu
 2. Press <ENTER>
 3. Select General Resource reports, option 4
 4. Press <ENTER>
 5. Enter Extract on the COMMAND line, press <ENTER>
 6. Select Access List report, option 4
 7. Select the Batch option by changing the Batch/Online option to a B
 8. Enter the value CONSOLE on the CLASS field prompt
 9. Press <ENTER>
 10. On the Processing Options panel enter Y on Explode RACF Groups in access list after detail line
 11. Press <ENTER>
 12. Select S on the JCL Submit Processing
 13. Review report output and ensure the following items are in effect for all MCS consoles:
 - a. Each console defined in the **CONSOLxx** parmlib members is defined to RACF with a corresponding profile in the **CONSOLE** resource class.
 - b. Each **CONSOLE** profile is defined with **UACC(NONE)**.
 - c. The userid associated with each console has READ access to the corresponding resource defined in the **CONSOLE** resource class.
 - d. Access authorization for **CONSOLE** resources restricts READ access to z/OS systems programming personnel and/or operations staff.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

c) If all of the above in step 13 are true, there is NO FINDING.

d) If any of the above in step 13 are untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00294**

Default Severity: Category II

Display User CONSOLE and System Commands privilege information, as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select General Resource Profile, option 4,
- d) Press <ENTER>
- e) On the General Resource Reports screen, select Access List, option 4
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Profile field and enter CONSOLE
- h) Tab down to the Class field and enter TSOAUTH
- i) Press <ENTER>
- j) On the Processing Options panel, enter a Y next to 'Explode RACF groups in access list after detail line' prompt
- k) Press <ENTER>
- l) On the JCL Submit Processing screen, select S to submit the batch job
- m) Press <ENTER>
- n) Return to the Security Server Reports menu, select Profile reports, option 5
- o) Press <ENTER>
- p) On the Profile Reports menu, select OPERPARM, option 5 under User Segments.
- q) Press <ENTER>
- r) On the USER OPERPARM SEGMENT REPORT screen, tab down to the Batch/Online prompt and enter B for batch processing
- s) Press <ENTER>
- t) On the JCL Submit Processing screen, select S to submit the batch job
- u) Press <ENTER>
- v) Review Access List report for TSOAUTH class, User OPERPARM Segment report and Access List report for MVS* profiles in the OPERCMDS class generated in ACP00282, ensure the following are in effect:
 - a) On the class TSOAUTH Access List report, if the CONSOLE privilege is not defined to the TSOAUTH resource class, there is NO FINDING.
 - b) At the discretion of the IAO, users may be allowed to issues Z/OS system commands from a TSO session. With this in mind, ensure the following items are in effect for users granted the CONSOLE resource in the TSOAUTH resource class:
 - c) On the User OPERPARM Segment report, ensure userids are restricted to the **INFO** level on the **AUTH** parameter specified in the **OPERPARM** segment of their userid, under the Console Authority field header.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- d) On the OPERCMDS class Access List generated in ACP00282, ensure userids are restricted to READ access to the **MVS.MCSOPER.userid** resource defined in the **OPERCMD** resource class.
- e) On the class TSOAUTH Access List generated above, ensure userids and/or group IDs are restricted to READ access to the **CONSOLE** resource defined in the **TSOAUTH** resource class.

If all of the above in (2) are true, there is NO FINDING.

If any of the above in (2) are untrue, this is a FINDING.

- w) If all of the above in (v) are true, there is NO FINDING
- x) If any of the above in (v) is untrue, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00320**

Default Severity: Category II

Audit Log - Daily Review

At a Minimum Weekly Review for the z/OS Level:

If the installation has the Vanguard Advisor product, run the Violation Detail report by selecting option 1 on the Advisor Main menu and then option 10, Violations Detail Report for Access Violations.

For invalid password attempts run Option 1 Standard Reports and then, Option 3 System Entry Summary Report. Hit enter for online report with No Masking specified. Look at the counts under the column Vios for the number of invalid logon attempts. Place an S next to any userid with Vios and review.

Look specifically for the following:

- a) A User attempting to read/update/delete/scratch/alter a critical dataset which the STIG prohibits:
 - 1. Security database files, and security setup (parmlib)
 - 2. System parmlib such as SYS1.PARMLIB
- b) A user generating violation(s) while attempting to update (or greater level) operating system datasets which they do not have access to:
 - 1. SYS1*, SYS2*, SYS3*, SYS4*, SYS*
- c) A user generating violation(s) while attempting to update (or greater level) APF libraries.
- d) A user generating violation(s) while attempting Volume Level access.
- e) Violations of JESSPOOL resources against domain level operations batch processing, system programmer submitted jobs, security related batch jobs and system level started tasks.
- f) Violations generated against critical system level resources FACILITY/IBMFAC and OPERCMDS.
- g) A review of users who incurred more than 10 password violations within a given day during the prior week – as an indicator for further review and research of possible unusual activity.
- h) The site may choose to monitor, at the discretion of the site, any additional critical system level resources they deem necessary above and beyond the above specified.

If any of the above unusual or inappropriate activity is found within the Audit Log records and documentation (email strings or other written documentation) exists showing actions were taken based upon the discovery of an unusual or inappropriate activity event, there is NO FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

If any of the above unusual or inappropriate activity is found within the Audit Log records and NO documentation exists, this is a FINDING

CCI: CCI-000148

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ACP00330

Default Severity: Category II

The IAO will provide a list of all userids that are shared among multiple users(i.e not uniquely identified system users).

- b) If there are no shared userids on this domain, there is NO FINDING.
- c) If there are shared userids on this domain, this is a FINDING.

NOTE: Userids should be able to be traced back to a current DD2875 or a Vendor Requirement (example: A Started Task).

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00340**

Default Severity: Category II

a) The z/OS Baseline reports (as identified by report/function CS221C and CS243C) shall be reviewed and validated with the appropriate system programming staff on the period of time required by the current INFOCON level.

The first time you run this analysis, follow these steps to create a baseline:

1. Gather information on APF libraries: From the Analyzer Main Menu, choose Option 4 Batch reports and then I Link Pack Area Analysis. Put an S next to Authorized Program Facility (APF) Table. Make sure AC(1) module List is set to YES and all other OPTIONS are NO. Hit Enter, Choose S to submit the JCL.
2. Gather information on LPA libraries: From the Analyzer Main Menu, choose Option 4 Batch reports and then OPTION B Sensitive/Critical Data Sets Analysis. Put an S next to Authorized Program Facility (APF) Table. Make sure all other OPTIONS are NO. Hit Enter, Choose S to submit the JCL.
3. Now, create a copy of these reports for future reference. Find the jobs on the spool, put a ? next to the job and then XDC next to the DDNAME REPORT. Fill in the information for the output dataset naming the APF library Report with the last qualifier of CS221C and the LPA report with the last qualifier of CS243C.

The second and subsequent times you run this analysis (step 1 and 2 above) and compare the new reports with the previously generated reports.

Look for the following and validate that any changes are valid. If changes were made that are valid, repeat steps 1-3 above to create a new baseline.

APF library stats (# of libraries in APF list, # duplicate libraries in APF list, # accessible of libraries in APF list, # of members in APF libraries, # of members linked with AC=1, # of APF libraries in LINKLIST/LPA, # duplicate of APF libraries in LINKLIST/APF, # of accessible APF libraries in LINKLIST/LPA, # of members in authorized LINKLIST/LPA, # of members links AC=1 in LINKLIST/LPA, total # of APF libraries, total # of unique APF libraries , total # of members with AC=1, total % of members with AC=1, APF datasets. This functional name will correspond to the dataset report file name that ends in CS221C .

LPA library display (LPA libraries added/removed, last accessed date for LPA libraries). This functional name will correspond to the dataset report file name that ends in CS243C .

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

Reports shall be compared with known and authorized changes to the specific z/OS domain. Any anomalies found shall be documented as a potential incident and must be investigated with written documentation as proof showing such review was completed.

b) If the baseline reports are being reviewed and samples of the reports exist, there is NO FINDING.

c) If the baseline reports are not being reviewed or samples of the reports do not exist this is a FINDING.

CCI: CCI-000294

CCI: CCI-000295

CCI: CCI-000296

CCI: CCI-001819

CCI: CCI-001823

CCI: CCI-002087

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ACP00350**

Default Severity: Category II

Note: Generic profiles can be used (i.e. IEA*.* instead of IEASYMUP.*) for the checks below, as long as all the detailed requirements re access and logging as specified below, are met.

Ensure the following are in affect:

- a) A covering profile for IEASYMUP.* exists and is defined with
UACC(NONE)
and AUDIT is specified as SUCCESSES(UPDATE) and FAILURES(READ)
- b) Only systems programmers, DASD Administrators and Tape Librarians are in the access list with UPDATE access or higher.
- c) To verify –
 - 1. From the Administrator Main Menu Choose Option 3;4 (Security Server Reports, General Resource Profiles)
 - 2. Tab down to CLASS and enter 'FACILITY '
 - 3. Tab down PROFILE and enter IEA*
 - 4) Find the covering profile for IEASYMUP.* and type LR next to it in the command line.
 - 5) Review the output against the requirements in a. above...
- d) If all of the above are TRUE, there is NO FINDING.
- e) If either
 - a covering profile is not found or
 - audit logging per above (SUCCESSES (UPDATE), FAILURES(READ)) is not specified or
 - personnel other than Systems Programmers have UPDATE or higher access then , there is a FINDING.

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0244**

Default Severity: Category II

Display Resource Class Information as follows:

- a) From Administrator main menu, select Security Server Commands,
- b) Press <ENTER>
- c) Select SETROPTS option 5 SETROPTS option,
- d) Press <ENTER>
- e) On the SETROPTS screen, locate the CDT Classes prompt, enter 'E' next to it.
- f) Press <ENTER>
- g) Invoke the locate command, Locate FACILITY
- h) Screen print the display showing the attributes of the FACILITY class, including active status
 - 1. If the FACILITY class is ACTIVE there is NOFINDING
 - 2. If the FACILITY class is not ACTIVE there is a FINDING
- i) If Item 1 is true then there is NOFINDING
- j) If Item 2 is true then there is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0246

Default Severity: Category II

Display Resource Class Information as follows:

- a) From Administrator main menu, select Security Server Commands,
- b) Press <ENTER>
- c) Select SETROPTS option 5 SETROPTS option,
- d) Press <ENTER>
- e) On the SETROPTS screen, locate the CDT Classes prompt, enter 'E' next to it.
- f) Press <ENTER>
- g) Invoke the locate command, Locate OPERCMDS
- h) Screen print the display showing the attributes of the OPERCMDS class, including active status
 - 1. If the OPERCMDS class is ACTIVE there is NOFINDING
 - 2. If the OPERCMDS class is not ACTIVE there is a FINDING
- i) If Item 1 is true then there is NOFINDING
- j) If Item 2 is true then there is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0248

Default Severity: Category II

Display Resource Class Information as follows:

- a) From Administrator main menu, select Security Server Commands,
- b) Press <ENTER>
- c) Select SETROPTS option 5 SETROPTS option,
- d) Press <ENTER>
- e) On the SETROPTS screen, locate the CDT Classes prompt, enter 'E' next to it.
- f) Press <ENTER>
- g) Invoke the locate command, Locate CONSOLE
- h) Screen print the display showing the attributes of the CONSOLE class, including active status
 - 1. If the CONSOLE class is ACTIVE there is NOFINDING
 - 2. If the CONSOLE class is not ACTIVE there is a FINDING
- i) If Item 1 is true then there is NOFINDING
- j) If Item 2 is true then there is a FINDING

CCI: CCI-000213

CCI: CCI-002233

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0250

Default Severity: Category II

Display Resource Class Information as follows:

- a) From Administrator main menu, select Security Server Commands,
- b) Press <ENTER>
- c) Select SETROPTS option 5 SETROPTS option,
- d) Press <ENTER>
- e) On the SETROPTS screen, locate the Dataset Options heading by using the PF8 key to scroll down the screen display
- f) Screen print the display showing the ADSP attributes under the Dataset Options heading, located on the right hand side of the screen.
 - 1. If the ADSP value shows as N , there is NOFINDING
 - 2. If the ADSP value shows as Y , this is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0260**

Default Severity: Category II

- a) In TSO Issue the SETR LIST command
- b) Capture from the Screen all the CLASSES LISTED next to AUDIT=
- c) Capture from the Screen all the CLASSES LISTED next to AUDIT=
- d) If all ACTIVE classes are also listed under the AUDIT classes, there is NO FINDING
- e) If any ACTIVE classes are not listed under the AUDIT classes, this is a FINDING.

CCI: CCI-001845

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0270

Default Severity: Category II

Display Resource Class Information as follows:

- a) Is ISPF 6, run SETR LIST
- b) Press <ENTER>
- c) Continue to press <ENTER> until the ACTIVE CLASSES heading appear, screen print the area where the TEMPDSN class are present.
 - 1. If TEMPDSN class listed is active (i.e. in the ACTIVE CLASS list) , there is NOFINDING
 - 2. If TEMPDSN class listed is not active (i.e. Not in the ACTIVE CLASS list), this is a FINDING

CCI: CCI-000213

CCI: CCI-002262

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0280

Default Severity: Category II

Display Resource Class Information as follows:.

- a) From Administrator main menu, select Security Server Commands,
 - 1. Press <ENTER>
 - 2. Select SETROPTS option 5 SETROPTS option,
 - 3. Press <ENTER>
 - 4. On the SETROPTS screen, locate the CMDVIOL field prompt, on the right hand side of the screen by the Auditing options.
- b) Screen print the display showing the value of the CMDVIOL attribute.
 - 1. If the CMDVIOL value is set to Y, there is NOFINDING
 - 2. If the CMDVIOL value is set to N, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-002723

CCI: CCI-002724

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0290**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the Dataset Options data area and locate the EGN field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the EGN attribute.
 - 1. If the EGN value is set to Y, there is NO FINDING
 - 2. If the EGN value is set to N, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000336

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0300

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the Dataset Options data area and locate the ERASE and ERASEALL field prompts.
- b) Screen print the display showing the value of the ERASEALL attribute.
 - 1. For both CLASSIFIED and CONFIDENTIAL systems and UNCLASSIFIED systems, if the ERASEALL value is set to Y, there is NO FINDING.
- c) For Classified and Confidential systems and Unclassified systems if b)1. above is true there is NO FINDING, otherwise there is a FINDING

CCI: CCI-001090

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0310**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Analyzer main Menu, go to option 4
 - 2. Press <ENTER>
 - 3. Select option 1 - Class Descriptor Table Analysis
 - 4. Press <ENTER>
 - 5. On the next screen, specify YES for Sort Criteria
 - 6. Press <ENTER>
 - 7. On the Sort Selection screen, enter a 1 next to the CMDS field name and a D for descending sequence. This will list the classes where Generic commands are not allowed first. Or if you prefer you could list them in ascending sequence and get the class where Generic commands are allowed first.
 - 8. Press <ENTER>
 - 9. On the JCL Submit Processing panel, select 'S' to submit the job
- b) Review Class Descriptor Table Analysis Report output for the classes in question.
 - 1. If the classes listed have Generics allowed YES as characteristic (except for those listed below) there is NO FINDING
 - 2. If the classes listed have Generics Allowed NO (that is not an exception), this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

Exceptions:

CDT
KERBLINK
REALM
SECLABEL
SECLMBR
USER
GROUP
DIGTCERT
DIGTRING
BCICSPCT
DIMS
ECICSDCT
GCICSTRN
GCPSMOBJ
GCSFKEYS
GDASDVOL
GDSNBP
GDSNCL
GDSNDB
GDSNJR
GDSNPK
GDSNPN
GDSNSC
GDSNSG
GDSNSM
GDSNSP

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

GDSNSQ
GDSNTB
GDSNTS
GDSNUF
GDSNUT
GEJBROLE
GIMS
GINFOMAN
GLOBAL
GMQADMIN
GMQCHAN
GMQNLIST
GMQPROC
GMQUEUEUE
GMXADMIN
GMXNLIST
GMXPROC
GMXQUEUEUE
GMXTOPIC
GSDSF
GSOMDOBJ
GTERMINL
GXFACILI
HCICSFCT
HIMS
JIMS
KCICSJCT
MIMS
NCICSPPT
NODES ** should not be excluded.
PROGRAM
QCICSPSB
QIMS
RACFVARS
SECDATA
SECLABEL
UCICSTST
UIMS
VCICSCMD
VMXEVENT
WCICSRES
WIMS
DIRACC
DIRAUTH
DIRSRCH
FSOBJ
FSSEC
IPCOBJ
PROCACT
PROCESS
TEMPDSN
VMMAC

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0320**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Analyzer main Menu, go to option 4
 - 2. Press <ENTER>
 - 3. Select option 1 - Class Descriptor Table Analysis
 - 4. Press <ENTER>
 - 5. On the next screen, keep YES for Sort Criteria
 - 6. Press <ENTER>
 - 7. On the Sort Selection screen, enter a 1 next to the ACTIVE field name and a D for descending sequence. This will list the classes where Generic profile checking is not active. Or if you prefer you could list them in Ascending sequence and get the class where Generic profile checking is active first.
 - 8. Press <ENTER>
 - 9. On the JCL Submit Processing panel, select 'S' to submit the job
- b) Review Class Descriptor Table Analysis Report output for the classes in question.
 - 1. GENERIC(*) must be specified on all CDT entries with the exception of CDT, DIGTCERT, DIGTRING, DIRACC, DIRAUTH, DIRSRCH, FSOBJ, FSSEC, IPCOBJ, PROCACT, PROCESS, TEMPDSN, VMMACCICSSMD, GLOBAL, KERBLINK, REALM and ALL group Resource classes (e.g., GCICSTRN, GDASDCOL, etc)
 - 2. If the GENERIC(*) is not on all CDT entries except CDT, DIGTCERT, DIGTRING, DIRACC, DIRAUTH, DIRSRCH, FSOBJ, FSSEC, IPCOBJ, PROCACT, PROCESS, TEMPDSN, VMMACCICSSMD, GLOBAL, KERBLINK, REALM and ALL group Resource classes (e.g., GCICSTRN, GDASDCOL, etc) values, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0330**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the UserID Options area and locate the TERMINAL field prompt, on the left hand side of the screen.
- b) Screen print the display showing the value of the TERMINAL attribute.
 - 1. If the TERMINAL value is set to READ, there is NO FINDING
 - 2. If the TERMINAL value is not set to READ, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-001958

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0350**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the UserID Options area and locate the GRPLIST field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the GRPLIST attribute.
 - 1. If the GRPLIST value is set to Y, there is NO FINDING
 - 2. If the GRPLIST value is not set to Y, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0360

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the UserID Options area and locate the INACTIVE field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the INACTIVE attribute.
 - 1. If the INACTIVE value is between 1 and 35, there is NO FINDING
 - 2. If the INACTIVE value is 0 or greater than 35, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000017

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0370**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the UserID Options area and locate the INITSTATS field prompt, on the left hand side of the screen.
- b) Screen print the display showing the value of the INITSTATS attribute.
 - 1. If the INITSTATS value is set to Y, there is NO FINDING
 - 2. If the INITSTATS value IS NOT set to Y, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000130

CCI: CCI-000131

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0380

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the UserID Options area and locate the JES(BATCHALLRACF) field prompt, under JES on the left hand side of the screen.
- b) Screen print the display showing the value of the JES(BATCHALLRACF) attribute.
 - 1. If the JES(BATCHALLRACF) IS SET TO y, there is NO FINDING
 - 2. If the JES(BATCHALLRACF) value is NOT SET to Y, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000764

CCI: CCI-002233

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0400**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, page down to the UserID Options area and locate the XBMALLRACF field prompt, under JES on the left hand side of the screen.
- b) Screen print the display showing the value of the JES(XBMALLRACF) attribute.
 - 1. If the JES(XBMALLRACF) value is set to Y, there is NO FINDING
 - 2. If the JES(XBMALLRACF) value is not set to Y, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000764

CCI: CCI-002233

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0420**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, locate the OPERAUDIT field prompt, under Auditing Options on the left hand side of the screen.
- b) Screen print the display showing the value of the OPERAUDIT attribute.
 - 1. If the OPERAUDIT value is set to Y, there is
NO FINDING
 - 2. If the OPERAUDIT value is not set to Y,
this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-002234

CCI: CCI-002262

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0430**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Password Options area and locate the HISTORY field prompt, on the left hand side of the screen.
- b) Screen print the display showing the value of the PASSWORD(HISTORY) attribute.
 - 1. If the PASSWORD(HISTORY) value is 10 or greater, there is NO FINDING
 - 2. If the PASSWORD(HISTORY) value is not at least 10, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000200

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0440**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Password Options area and locate the INTERVAL field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the PASSWORD(INTERVAL) attribute.
 - 1. If the PASSWORD(INTERVAL) value is less than or equal to 60 and not 0, there is NO FINDING
 - 2. If the PASSWORD(INTERVAL) value is 0 or greater than 60, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000199

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0445**

Default Severity: Category I

- a) Display the Password Minimum Change Interval Information as follows:
 - 1. From Administrator main menu, select Security Server Commands, option 2.
 - 2. Press <ENTER>
 - 3. From the VRC main menu, select SETROPTS option 5
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Password Options area and locate the MIN INTERVAL field prompt, on the right hand side of the screen.
- b) If the PASSWORD(MIN INTERVAL) greater than 0 and less than or equal to 59, there is NO FINDING
- c) If the PASSWORD(MIN INTERVAL) value is 0 or greater than 59, this is a FINDING.

CCI: CCI-000198

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0450**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Password Options area and locate the REVOKE field prompt, on the left hand side of the screen.
 - 6. On the SETROPTS screen, scroll down to the UserID Options area and ensure that Initstats is set to Y
- b) Screen print the display showing the value of the PASSWORD(REVOKE) attribute.
 - 1. If the PASSWORD(REVOKE) value is set to either 1 or 2, and Initstats is set to Y, there is NO FINDING
 - 2. If the PASSWORD(REVOKE) value is not set to either 1 or 2, or Initstats is set to N, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000044

CCI: CCI-002238

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0460

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Password Options area and locate the RULE field prompt, on the right hand side of the screen.
 - 6. Enter E next to the Rule field prompt to display Rule definitions.
- b) Screen print the display showing the value of the PASSWORD(RULEn) attribute.
 - 1. If the PASSWORD(RULEn) value conforms to at least one of the following:
 - RULE 1 LENGTH(8) \$mmmmmmmm
 - RULE 2 LENGTH(8) m\$mmmmmmmm
 - RULE 3 LENGTH(8) mm\$mmmmmm
 - RULE 4 LENGTH(8) mmm\$mmmmmm
 - RULE 5 LENGTH(8) mmmm\$mmmmmm
 - RULE 6 LENGTH(8) mmmmm\$mmmmmm
 - RULE 7 LENGTH(8) mmmmmmm\$mmmmmm
 - RULE 8 LENGTH(8) mmmmmmmmm\$, there is NO FINDING
 - 2. If the PASSWORD(RULEn) value does not conform to at least one of the above rules, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000205

CCI: CCI-001619

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0462**

Default Severity: Category II

The RACF exit ICHPWX01 will allow for additional checks not available in RACF SETROPTS whenever a user selects a new password.

- a) From system console type command **F AXR,IRRPWREX LIST**
- b) Review results of system console modify command for the following
 1. The number of required character types is 4 (assures that at least 1 upper, 1 lower, 1 number, and 1 special character is used in password)
 2. The user's name cannot be contained in the password
 - a. Only 3 consecutive characters of the user's name are allowed
 - b. The minimum word length checked is 8
 3. The user ID cannot be contained in the password
 - a. Only 3 consecutive characters of the user ID are allowed
 4. Only 3 unchanged positions of current password allowed
 - a. Positions need to be consecutive to cause a failure
 - b. Check is not case sensitive
 5. No more than 0 pairs of repeating characters are allowed
 - a. Check is not case sensitive
 6. A minimum list of 33 restricted prefix strings is being checked

APPL	APR
AUG	ASDF
BASIC	CADAM
DEC	DEMO
FEB	FOCUS
GAME	IBM
JAN	JUL
JUN	LOG
MAR	MAY
NET	NEW
NOV	OCT
PASS	ROS
SEP	SIGN
SYS	TEST
TSO	VALID
VTAM	XXX
1234	

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- c) If the modify command fails or returns message “IRX0406E REXX exec load file REXXLIB does not contain exec member IRRPWREX” in the system log, this is a FINDING.
- d) If the above message does not appear in the system log and no failure of the modify command, there is NO FINDING.

CCI: CCI-000192

CCI: CCI-000193

CCI: CCI-000194

CCI: CCI-000195

CCI: CCI-000205

CCI: CCI-001619

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0465**

Default Severity: Category I

- d) Refer to the following report produced by the Data Set and Resource Data Collection:

SENSITIVE.RPT(RACFREXX)

OR

- e) Refer to the zOS system REXXLIB concatenation found in SYS1. PARMLIB (AXR) for the data set that contains the REXX for Password exit named IRRPWREX and the defined AXRUSER.
- f) Verify that the data set that contains IRRPWREX is properly restricted. If the following guidance is true, this is NOT A FINDING.
- 1) RACF data set access authorizations restrict READ to AXRUSER, z/OS systems programming personnel, security personnel, and auditors.
 - 2) RACF data set access authorizations restrict UPDATE to security personnel using a documented change management procedure to provide a mechanism for access and revoking of access after use.
 - 3) All (i.e., failures and success) data set access authorities (i.e., READ, UPDATE, and CONTROL) is logged
 - 4) RACF data set access authorizations specify UACC(NONE) and NOWARNING.
- g) If any of the above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

CCI: CCI-002357

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0467**

Default Severity: Category I

- a) From the ISPF Command Shell enter

SETRopts List

OR

- b) Refer to the following report(s) produced by the RACF Data Collection:

RACFCMDS.RPT(SETROPTS)

or

PDI(RACF0467) (Automated Analysis)

- c) If the following is specified under PASSWORD PROCESSING OPTIONS:
“THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES”, this
is not a Finding.

CCI: CCI-002450

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: RACF0470

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Password Options area and locate the WARNING field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the PASSWORD(WARNING) attribute.
 - 1. If the PASSWORD(WARNING) value is greater than or equal to 10, there is NO FINDING
 - 2. If the PASSWORD(WARNING) is less than 10, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-001395

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0480**

Default Severity: Category I

Display Resource Class Information as follows:

- a) From Administrator main menu, select Security Server Commands,
 1. Press <ENTER>
 2. Select SETROPTS option 5 SETROPTS option,
 3. Press <ENTER>
 4. On the SETROPTS screen, scroll down to the Dataset Options area and locate the PROTECTALL field prompt, on the left hand side of the screen.
- b) Screen print the display showing the value of the PROTECTALL attribute.
 1. If the **SETROPTS PROTECTALL** is set to PROTECTALL or PROTECTALL(FAILURE), there is NO FINDING.
 2. If the **SETROPTS PROTECTALL** parameter is set to **NOPROTECTALL** or **PROTECTALL(WARNING)**, this is a FINDING. Additional analysis may be required to determine whether this FINDING should be downgraded to a Category II or remain a Category I. Clear and specific documentation must be provided justifying the downgrade to a Category II.
 - a. Example of a Category I FINDING where **no** further analysis is required:
 1. Control Options: **SETROPTS NOPROTECTALL**
 - b. Example of a possible Category I FINDING requiring additional analysis:
 1. Control Options: **SETROPTS PROTECTALL (WARNING). PROTECTALL(WARNING)** allows access to a data set only if it is not protected by a profile in the **DATASET** resource class. Therefore if all sensitive data sets are properly protected by profiles in the **DATASET** resource class, **PROTECTALL(WARNING)** will not allow unauthorized access. This situation would justify a downgrade to a Category II.
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0490**

Default Severity: Category III

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Dataset Options area and locate the REALDSN field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the REALDSN attribute.
 - 1. If the REALDSN value is set to Y, there is NO FINDING
 - 2. If the REALDSN value is not set to Y, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-001353

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0500**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Dataset Options area and locate the RETPD field prompt, on the left hand side of the screen.
- b) Screen print the display showing the value of the RETPD attribute.
 - 1. If the RETPD is set to 99999 (which means it never expires), there is NO FINDING
 - 2. If the RETPD is not set to 99999, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0510**

Default Severity: Category II

- a) Go to option TSO and execute a SETROPTS LIST
- b) If the "INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT" message for both the SWITCH and STATUS functions and conforms to PASSWORD CONTENT requirements as documented in RACF0460, there is NO FINDING.
- c) If the "INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT" message for both the SWITCH and STATUS functions but does not conform to PASSWORD CONTENT requirements as documented in RACF0460, this is a FINDING.
- d) If the "DEFAULT RVARY PASSWORD IS IN EFFECT" message for the SWITCH or STATUS functions, this is a FINDING.

CCI: CCI-001813

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0520**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, locate the SAUDIT field prompt, on the left hand side of the screen under Auditing options.
- b) Screen print the display showing the value of the SAUDIT attribute.
 - 1. If the SAUDIT values is set to Y, there is NO FINDING
 - 2. If the SAUDIT values is set to N, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000172

CCI: CCI-002724

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0540**

Default Severity: Category III

- a) In TSO Issue the SETR LIST command
- b) Capture from the Screen all the CLASSES LISTED next to LOGOPTIONS "FAILURES" CLASSES=
- c) Capture from the Screen all the CLASSES LISTED next to ACTIVE=
- d) If all ACTIVE classes are also listed under the LOGOPTIONS "FAILURES" CLASSES= classes, there is NO FINDING
- e) If any ACTIVE classes are not listed under the LOGOPTIONS "FAILURES" CLASSES= classes, this is a FINDING.
- f) LOGOPTIONS "NEVER" CLASSES = NONE is specified, then NO FINDING otherwise FINDING

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0550**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Dataset options area and locate the TAPEDSN field prompt, on the right hand side of the screen.
- b) Screen print the display showing the value of the TAPEDSN attribute.
 - 1. If the TAPEDSN value is set to Y, there is NO FINDING
 - 2. If the TAPEDSN value is set to N, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0560**

Default Severity: Category II

- a) Display Resource Class Information as follows:
 - 1. From Administrator main menu, select Security Server Commands,
 - 2. Press <ENTER>
 - 3. Select SETROPTS option 5 SETROPTS option,
 - 4. Press <ENTER>
 - 5. On the SETROPTS screen, scroll down to the Dataset options area and locate the PROGRAM field prompt, under WHEN on the left hand side of the screen.
- b) Screen print the display showing the value of the WHEN(PROGRAM) attribute.
 - 1. If the WHEN(PROGRAM) is set to Y,
there is NO FINDING
 - 2. If the WHEN(PROGRAM) values is not set to Y, this is a FINDING
- c) If Item (b.1) is true then there is NO FINDING
- d) If Item (b.2) is true then there is a FINDING

CCI: CCI-000366

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0570**

Default Severity: Category III

Display User ID Information as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select User Profile, option 1,
- d) Press <ENTER>
- e) On the User Reports screen, select User Summary, option 1,
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Press <ENTER>
- h) On the JCL Submit Processing screen, select S to submit the batch job
- i) Review User Summary report output and ensure that the following items are in effect for all users including batch userids:
 - 1. A completed NAME field that can either be traced back to a current DD2875 or a Vendor Requirement (example: A Started Task).
 - 2. The presence of the DEFAULT-GROUP and OWNER fields.
 - 3. The PASSDATE field is not set to N/A unless this user has the PROTECTED attribute
- j) If (i) any of the above is untrue, this is a FINDING.

CCI: CCI-000764

CCI: CCI-000804

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0580**

Default Severity: Category II

Note: Current DoD policy has changed requiring that the password change interval be at the most 60 days. Ensure that this is in effect.

Note: FTP only process and server to server userids may have PASSWORD(NOINTERVAL) specified. These users must be identified in the FTPUSERS group in the Dialog Process or FTP in the name field. Additionally these users must change their passwords on an annual basis.

- a) Ensure that PASS-INTERVAL is a value of 1 to 60 days.
 - 1. From the Vanguard Administrator main menu enter 2;5 to enter Vanguard RACF Commands panel.
 - 2. Scroll to the area marked Password Options and verify that interval is set between 1 to 60 days inclusive.
 - 3. From the Vanguard Administrator main menu enter 3;1 to enter the User Reports panel.
 - 4. Enter Y in the enhanced masking field of this panel and press enter.
 - 5. On the enhanced command line enter PWDINTERVAL GE 61 and press enter.
 - 6. If any list results this is a FINDING. Indicates these user ids do not have a password interval set from 1 to 60.
- b) Ensure that the following items are in effect for Interactive users (non-batch only or STC protected users):
 - 1. No userid has the LAST-ACCESS field set to UNKNOWN.
 - a. From the Vanguard Administrator main menu enter 3;1.
 - b. Press enter at the User Summary panel to list all RACF defined user ids.
 - c. From the resulting display enter sort racinit on the command line and press enter. The display will be sorted in descending order.
 - c) If a(6) list is blank and b(g) is true there is NO FINDING.
 - d) If a(6) list is not blank, b(g) is untrue, this is a FINDING.

CCI: CCI-000199

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0590**

Default Severity: Category II

Refer to the following item in Appendix B, Preliminary Worksheet (Part 2 of 2):

- Item 11

Display SURROGAT resource class information, as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select General Resource Profile, option 4,
- d) Press <ENTER>
- e) On the General Resource Reports screen, select Access List, option 4
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Class field and enter SURROGAT
- h) Press <ENTER>
- i) On the Processing Options panel, enter a Y next to 'Explode RACF groups in access list after detail line' prompt
- j) Press <ENTER>
- k) On the JCL Submit Processing screen, select S to submit the batch job
- l) Press <ENTER>
- m) If the submission of batch jobs via an automated process (e.g. job scheduler, job submission started task, etc.) is being utilized, ensure the following items are in effect:

1. The SURROGAT resource class is active. Note: This does not need to be checked, automation check is performed in ZUSSR060.

2. On the SURROGAT class Access List report, ensure each batch job userid used for batch submission by a job scheduler (e.g., CONTROL-M, CA-7, CA-Scheduler, etc.) is defined as an execution-userid in a SURROGAT RESOURCE CLASS profile. For example:

RDEFINE SURROGAT execution-userid.SUBMIT
UACC(NONE) OWNER(execution-userid)

3. On the SURROGAT class Access List report, ensure each job scheduler useid (i.e. surrogate-userid) is permitted surrogate activity to the appropriate SURROGAT profiles. For example:

PERMIT execution-userid.SUBMIT CLASS(SURROGAT)
ID(surrogate-userid) ACCESS(READ)

- n) If all of the above in (m) are true, there is NO FINDING

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- o) If any of the above in (m) is untrue, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0595**

Default Severity: Category II

Refer to the following item in Appendix B, Preliminary Worksheet (Part 2 of 2):

- Item 11

Display User ID Information as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select User Profile, option 1,
- d) Press <ENTER>
- e) On the User Reports screen, select User Summary, option 1,
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab to the Protected field and type Y for protected
- h) Press enter
- i) On the JCL Submit Processing screen, select S to submit the batch job
- j) Review User Summary report output and ensure that the following items are in effect for batch userids:
 - k) Press <ENTER>
 - l) On the JCL Submit Processing screen, select S to submit the batch job
 - m) Review User Summary report output and ensure that the following items are in effect for batch userids:
 1. All batch Userids have a NAME value displayed on the report. Also, the literal N/A shows under the Password Interval and Password Last Changed Date headings, this indicates they are PROTECTED Userids. If both these items are true there is NOFINDING.
 2. No batch Userid displays 'NEVER USED' under the Last RACINIT date, if this is true there is NOFINDING.
- n) If all of the above in (m) are true there is NOFINDING
- o) If any of the above in (m) is untrue, this is a FINDING

CCI: CCI-000052

CCI: CCI-000724

CCI: CCI-000764

CCI: CCI-000804

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0600**

Default Severity: Category II

Refer to the following items in Appendix B, Preliminary Worksheet (Part 2 of 2):

- Item 9: List of all Multiple User Access Systems in use on this system. These are systems that run in a single address space, but allow multiple users to sign on to them (e.g., CICS regions, Session Managers, etc.). For each region, also include corresponding userids, profiles, data management files, and a brief description (of each region).
- Item 11: Documentation of the process used for submission of batch jobs via an automated process (i.e., scheduler or other sources) and each of the associated userids.

Display PROPCNTL Resource Class Information as follows:

- a) From Administrator main menu, select Security Server Commands,
- b) Press <ENTER>
- c) Select SETROPTS (option 5),
- d) Press <ENTER>
- e) On the SETROPTS screen, locate the CDT Classes prompt, enter 'E' next to it.
- f) Press <ENTER>
- g) At the command prompt, invoke the locate command for PROPCNTL, type L PROPCNTL
- h) Screen print the display showing the attributes of the PROPCNTL class, including active status
- i) Return to the Administrator main menu and select Security Server Reports, option 3
- j) On the Security Server Reports menu, select General Resource Profile, option 4.
- k) On the General Resource reports screen, select General Resource Profile Summary, option 1
- l) Enter Extract on the COMMAND line, press <ENTER>
- m) Tab down to the Batch/Online prompt and enter B to generate a batch job
- n) Tab down to the Class field and enter PROPCNTL
- o) Press <ENTER>
- p) On the JCL Submit Processing screen, select S to submit the batch job
- q) Press <ENTER>
- r) If (1) the submission of batch jobs via an automated process (e.g. job scheduler, job submission started task, etc.) is being utilized, and/or (2) Multiple User Single Address Space Systems (MUSASS) capable of submitting batch jobs are active on this system, ensure the following items are in effect:

1. The PROPCNTL resource class is active, as displayed on the Security Server Commands CDT screen print.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

2. On the class PROPCNTL General Resource Profile Summary report, ensure a PROPCNTL resource class profile is defined for each userid associated with a job scheduler (e.g. CONTROL-M, CA-7, etc.) and a MUSASS able to submit batch jobs (e.g., CA-ROSCOE, etc.)

s) If both of the above in (r) are true, there is NO FINDING

t) If either of the above in (r) is untrue, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0620**

Default Severity: Category II

Refer to the following items in APPENDIX B, Preliminary Worksheet (Part 1 of 2):

- Item 2
 - a) Display STARTED class information as follows:
 1. From Analyzer main Menu, go to option 4
 2. Press <ENTER>
 3. Select option 4 - Started Procedures Analysis
 4. Press <ENTER>
 5. On the next screen, keep YES for Sort Criteria
 6. Press <ENTER>
 7. On the Sort Selection screen, enter a 1 next to the USERID field name
This will list Started Procedure information in Userid order.
 8. Press <ENTER>
 9. On the JCL Submit Processing panel, select 'S' to submit the job
 - b) Review Started Procedures Analysis Report output looking for userids associated with multiple started procedures as well as started procedure names containing an * in the Procname, which indicates there might be multiple Started procedures sharing this userid.

NOTE: For Vendor Products, STC userids are allowed to be unique per product and function if supported by vendor documentation.

- c) If all started task procedures have a unique associated userid, there is NO FINDING.
- d) If any started task procedure does not have a unique associated userid, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0650**

Default Severity: Category II

Refer to the following items in APPENDIX B, Preliminary Worksheet (Part 1 of 2):

- Item 2

I. STC Group ID's

Display STARTED class information as follows:

- a) Refer to Started Procedures Analysis report in RACF0620.
- b) Review Started Procedures Analysis Report output looking for finding messages related to 'Group ID not defined to RACF' or 'Userid not connected to Group' or 'UserID not defined to RACF'.
 1. If none of the above is true, there is NO FINDING.
 2. If any of the above is true, this is a FINDING.
- c) Generate Profile Segments Report
 1. In Administrator, select option 3 on the main menu
 2. Press <ENTER>
 3. Select Profile Segment reports, option 5
 4. Press <ENTER>
 5. Select STDATA report, option 41
 6. Press <ENTER>
 7. Select the Online option by changing the Batch/Online option to a O
 8. Select the Enhanced Masking function, enter the following criteria
GROUP NE spaces
 9. Press <ENTER>
 10. Run the STDATA report
 11. Sort display data on GROUP by entering the command SORT GROUP on the command prompt.
 12. Enter QG on the Command line
 13. Press <ENTER>
 14. On the QG edit panel, enter the following pattern:

REPORT(CONNECT SUMMARY)
GROUP(&GROUPID)
REPORT(END)

15. Invoke the GEN command,
16. Press <ENTER>
17. Delete duplicate group entries from generated Output.
18. Save data to a sequential dataset or PDS.
19. Return to Security Server Reports main menu by pressing PF3

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

20. Select Connect Reports option 15
21. Press <ENTER>
22. Select the Batch Option
23. Press <ENTER>
24. Select E on the JCL Submit Processing
25. Update the SYSIN JCL statement as follows:

```
//SYSIN DD DSN=YOUR.DATASET.NAME.FROM.QG.HERE,  
DISP=SHR
```

26. Submit report job by entering SUB on the command line
- d) Review report output searching for Userids connected to selected STC groups which are not STC userids.
 - e) If there are no userids connected to STC groups which are not STC userids, there is NO FINDING.
 - f) If there are userids connected to STC group which are not STC userids, this is a FINDING.
 - g) If items (b.1) and (e) are true then there is NO FINDING
 - h) If either (b.2) or (f) is true then there is a FINDING

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

II. STC Default Profile

Display STARTED class information as follows:

- a) Refer to Started Procedures Analysis report in RACF0620.
- b) Review Started Procedures Analysis Report output looking for a Procname of **, this should be at the top of the report list, there should be one present. If there is no ** Procname, this is a finding; otherwise, note the GroupID associated with the ** Procname entry.
- c) Generate Access Report
 - 1. In Administrator, select option 3 on the main menu
 - 2. Press <ENTER>
 - 3. Select ID In Access report, option 17
 - 4. Enter G on the ID Type prompt
 - 5. Enter Groupid associated with the ** Procname entry
 - 6. Select the Batch option by changing the Batch/Online option to a B
 - 7. Press <ENTER>
 - 8. Select S on the JCL Submit Processing
- d) Review report output searching for any access granted to explicit data set or resources. There should not be any.
- e) If both (b) and (d) are true, NO FINDING.
- f) If either (b) or (d) is true, this is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

III. ICHRIN03 Entries

Display STARTED class information as follows:

- a) Generate Started Procedures Analysis Report
 1. From Analyzer main Menu, go to option 4
 2. Press <ENTER>
 3. Select option 4 - Started Procedures Analysis
 4. Press <ENTER>
 5. On the next screen, keep YES for Sort Criteria
 6. Press <ENTER>
 7. On the Sort Selection screen, enter a 1 next to the SOURCE field name.
This will list Started Procedure information in Source order.
 8. Press <ENTER>
 9. On the JCL Submit Processing panel, select 'S' to submit the job
- b) Review Started Procedures Analysis Report output searching for Procname entries showing ICHRIN03 under the Source field heading. Critical Started Tasks should be supported by an ICHRIN03 entry.
- c) If (b) is true, there is NO FINDING.
- d) If (b) is not true, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0660**

Default Severity: Category II

- a) Display STARTED class information as follows:
 - 1. From Analyzer main Menu, go to option 3 - Online Displays
 - 2. Press <ENTER>
 - 3. Select option 4 - Started Procedures Analysis
 - 4. Press <ENTER>
- b) Review Started Procedures Analysis searching for STC definitions for the following:
 - 1. Review Started Procedures Analysis searching for STCs which show a Yes under the PRI field heading. Use SORT PRI to sort any with a Y to the bottom.
 - a. If any STC has a Y in the PRI column, there is a finding.
 - 2. Next, Review the Started Procedures for any STC definitions with Y in the TRU field (TRUSTED). Use SORT TRU on the command line to sort all the trusted STC's to the bottom.
 - a. Validate that only STCs in the list below have the TRUSTED attribute (ie, have a Y in the TRU column)
 - b. If additional STCs have the TRUSTED flag enabled, and documentation exists from DISA Field Security Operations approving the additional STCs, there is NO FINDING.
 - 3. Ensure that an entry ** exists and has no access or resources granted to it including a UACC of NONE.
 - a. To accomplish this go into ADMINISTRATOR, Option #4, On-line Access and Authorization, fill in these fields with the specified values and hit enter:
 - 1. CLASS..... : STARTED
 - 2. Resource Name (without quotes) .. **
 - 3. Access to check NONE
 - b. If the display field near the top left indicates that No Profile exists (see b.1 below for an example) this is a finding as the ** profile must exist.
 - 1. Profile: **No Profile exists**
 - c. On the screen that displays, CHECK that the UACC is NONE and that the ACCESS LIST that is displayed is NULL.
 - d. If any of the above is untrue, this is a FINDING..
- c) If All Started Procedures conform with 1.a, 2.a & 2.b, 3.b & 3.c, there is NO FINDING.

If any Started Procedure does not conform with 1.a, 2.a & 2.b, 3.b & 3.c., there is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

TRUSTED STARTED TASKS
ACF2
ACFBKUP
APSWPROA
APSWPROB
APSWPROC
APSWPROM
APSWPROT
CATALOG
CONSOLE
DFHSM*
DFS
DUMPSRV
GPMSEVERE
GSKSRVR
IEEVMPCR
IOSAS
IXGLOGR
JES2
JESXCF
LLA
NFS
OMVS/OMVSKERN***
RACF
RMF
RMFGAT
SMF
SMSRESTN
SMSRESTR
SMSVSAM
TCPIP
TSS
TSSB
TSSBKUP
TSSRESTN
VL
VTAM
XCFAS
ZFS**

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0680**

Default Severity: Category II

- Refer to U_zOS_STIG_INSTRUCTION.doc., Preliminary Worksheet (Part 2 of 2), Item 1: for data required for this check Item
- 1: All documents and procedures that apply to the following sections and/or units:
 - a. **Operations** Including system IPL procedures and SMF collection file backup specifics.
 - b. **Storage Management** Including identification of the DASD backup files and all associated storage management userids/LIDs/ACIDs.
 - c. **Security Management and Tracking**
 - d. **Change Management**

To display DASDVOL, GDASDVOL, FACILITY Resource Class and Userid Information, use Administrator for the following tasks:

1. Go to the Administrator Main Menu and select Security Server Reports, option 3
2. On the Security Server Reports menu, select General Resource Profile, option 4.
3. On the General Resource reports screen:
 - Select Access Lists, option 4; and
 - Tab down to the Batch/Online prompt and enter B to generate a batch job; and
 - Tab to the Enhanced Masking prompt and enter Y next to it
 - Press <ENTER>

Note: You may need to be in extract mode to complete this. Type in 'extract' at the command line, then <ENTER>, then enter the above screen.

4. On the Enhanced Masking panel enter the following masking string:

CLASS = DASDVOL OR CLASS=GDASDVOL

Note: If working with SMS-managed volumes, enter the following masking string instead:

CLASS=DASDVOL OR CLASS=GDASDVOL OR (CLASS=FACILITY
and PROFILE=STG*)

5. Press <ENTER>
6. On the Processing Options panel, enter Y by the prompt 'Explode RACF groups in access list after detail line'
7. Press <ENTER>
8. On the JCL Submit Processing screen, select S to submit the batch job
9. Press <ENTER>
10. Return to the Security Server Reports menu, select User Profile, option 1
11. Press <ENTER>
12. On the User Reports screen:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- Select User Summary, option 1
- Tab down to the Batch/Online prompt and enter B to generate batch job
- Tab Down to the Operations masking field and overwrite the * with a Y to list select userids with the operations attribute only
- Press <ENTER>

Note: You may need to be in extract mode to complete this. Type in 'extract' at the command line, then <ENTER>, then enter the above screen.

13. On the JCL Submit Processing screen, select S to submit the batch job
14. Press <ENTER>
15. Check the Access list report:
 - a) If batch userids assigned to storage maintenance tasks (e.g., volume backup, data set archive and restore, etc.) are given access to data sets using **DASDVOL** and/or **GDASDVOL** profiles, there is **NO FINDING**.
 - b) If working with SMS-managed volume, review access to **FACILITY** class, **STG*** profiles instead; if batch userids are given access to datasets using **FACILITY** class, **STG*** profiles, there is **NO FINDING**.

***NOTE: DASDVOL** profiles will not work with SMS-managed volume. **FACILITY** class profiles must be used instead. If DFSMS/MVS is used to perform DASD maintenance operations, **FACILITY** class profiles may also be used to authorize storage maintenance operations to non-SMS-managed volumes in lieu of using **DASDVOL** profiles. Therefore, not all volumes may be defined to the **DASDVOL/GDASDVOL** resource classes, and not all storage management userids may be represented in the profile access lists.*

16. Check the User Summary report. If any storage management userid is given the **OPERATIONS** attribute to perform DASD maintenance operations, this is a **FINDING**.
17. If the storage management userid is not defined with the **PROTECTED** attribute, this is a **FINDING**
18. If both of the above in (15) , (16) and (17) are true, there is **NO FINDING**
19. If either of the above in (15), (16) and (17) is untrue, this is a **FINDING**

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0690**

Default Severity: Category II

- a) Refer to U_zOS_STIG_INSTRUCTION.doc., Preliminary Worksheet (Part 2 of 2), Item 3: Item 3: Copies of all source, vendor integrity statements, or other documentation for all installed system, user, and ACP exits maintained by the site. Also include a list of the libraries in which these modules are contained
 - b) To get DASDVOL, GDASDVOL Resource Class and Userid Information, do the following tasks:
 1. Go to the Analyzer main menu, select option 4
 2. On the Batch Reports menu select TSO UADS, option U
Note: Analyzer 8.1 with PTF VS48081 is required for this option to be available.
 3. Press <ENTER>
 4. Set “Exceptions only” and “Sort Criteria” fields to NO.
 5. Press <ENTER>
 6. On the JCL Submit Processing menu, select S to submit the batch report
 7. Press <ENTER>
 8. Go to the Administrator main menu, select Security Server Reports, option 3
 9. On the Security Server Reports menu, select General Resource Profile, option 4.
 - a. On the General Resource reports screen:
 - b. Select Access Lists, option 4; and
 - c. Tab down to the Batch/Online prompt and enter B to generate a batch job; and
 - d. Tab to the Enhanced Masking prompt and enter Y next to it
 - e. Press <ENTER>
- Note: You may need to be in extract mode to complete this. Type in ‘extract’ at the command line, then <ENTER>, then enter the above screen.
10. On the Enhanced Masking panel enter the following masking string:
 11. CLASS = DASDVOL OR CLASS=GDASDVOL
 12. Press <ENTER>
 13. On the Processing Options panel, enter Y by the prompt ‘Explode RACF groups in access list after detail line’
 14. Press <ENTER>
 15. On the JCL Submit Processing screen, select S to submit the batch job
 16. Press <ENTER>
 17. Return to the Security Server Reports menu, select User Profile, option 1
 18. Press <ENTER>

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

19. On the User Reports screen, select User Summary, option 1
20. Tab down to the Batch/Online prompt and enter B to generate batch job
21. Press <ENTER>
22. On the JCL Submit Processing screen, select S to submit the batch job
23. Press <ENTER>
24. Ensure the following items are in effect regarding emergency userids:
 - a. Use the User Summary report to ensure userids exist to perform operating system functions **without** any RACF security administration privileges. These userids are defined to RACF with the **system-OPERATIONS** attribute, and FULL access to all DASD volumes. They must not have the **SPECIAL** attribute. Also, on the DASDVOL/GDASDVOL Access List report, ensure operating system function userids or any associated group are not in the access list of a resource profile.

NOTE: A user who has the system-OPERATIONS attribute has FULL access authorization to all RACF-protected resources in the DASDVOL/GDASDVOL resource classes. However, if their userid or any associated group (i.e., default or connect) is in the access list of a resource profile, they will only have the access specified in the access list.

- b. Check the User Summary report to ensure userids exist to perform RACF security administration **only**. These userids are defined to RACF with the **system-SPECIAL** attribute. They must not have the **OPERATIONS** attribute.
 - c. On the User Summary report, ensure all emergency userids are defined to RACF. Use the TSO UADS Analysis report to ensure all emergency userids are defined to SYS1.UADS.
- c) If all items (a,b,c) in (24) are true, there is NO FINDING.
- d) If any item in (24) is untrue, this is a FINDING.

CCI: CCI-000035

CCI: CCI-001220

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0710**

Default Severity: Category II

Display User ID Information as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select User Profile, option 1,
- d) Press <ENTER>
- e) On the User Reports screen, select User Summary, option 1,
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Masking Fields area of the screen and enter Y next to the Special prompt
- h) Press <ENTER>
- i) On the JCL Submit Processing screen, select S to submit the batch job
- j) Press <ENTER>
- k) Return to the Security Server Reports menu, select Connect Reports, option 15
- l) Press <ENTER>
- m) On the Connect Reports screen, select Connect Summary, option 1
- n) Tab down to the Batch/Online field, type a B (for batch)
- o) Tab down to the Masking Fields area of the screen and enter Y next to the Special prompt.
- p) Press <ENTER>
- q) On the JCL Submit Processing screen, select S to submit the batch job
- r) Press <ENTER>
- s) Review User Summary and Connect Summary report output and ensure that the following items are in effect regarding the SPECIAL and GROUP-SPECIAL attributes:
 - 1. Authorization to the SPECIAL or GROUP-SPECIAL attribute is restricted to security personnel.
 - 2. At minimum, ensure that any users connected to sensitive system dataset HLQ groups with the Group-SPECIAL attribute are security personnel. Otherwise, Group-SPECIAL is allowed.
- t) If both items in (s) are true there is NO FINDING.
- u) If either item in (s) is untrue, this is a FINDING

CCI: CCI-000035

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0720**

Default Severity: Category II

Display User ID Information as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select User Profile, option 1,
- d) Press <ENTER>
- e) On the User Reports screen, select User Summary, option 1,
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Masking Fields area of the screen and enter Y next to the Operations prompt
- h) Press <ENTER>
- i) On the JCL Submit Processing screen, select S to submit the batch job
- j) Press <ENTER>
- k) Return to the Security Server Reports menu, select Connect Reports, option 15
- l) Press <ENTER>
- m) On the Connect Reports screen, select Connect Summary, option 1
- n) Tab down to the Batch/Online field, type a B (for batch)
- o) Tab down to the Masking Fields area of the screen and enter Y next to the Operations prompt.
- p) Press <ENTER>
- q) On the JCL Submit Processing screen, select S to submit the batch job
- r) Press <ENTER>
- s) Review User Summary and Connect Summary report output and ensure that the following items are in effect regarding the OPERATIONS and GROUP-OPERATIONS attributes:

1. Authorization to the OPERATIONS or GROUP-OPERATIONS attribute is restricted to key systems personnel, such as individuals responsible for continuing operations and emergency recovery.

2. At minimum, ensure that any users connected to sensitive system dataset HLQ groups with the Group-OPERATIONS are key systems personnel, such as individuals responsible for continuing operations, Storage Management, and emergency recovery. Otherwise, Group-OPERATIONS is allowed.

NOTE: For sites running below RACF 2.1, the OPERATIONS attribute may be granted to STCs that do not require full TRUSTED status.

- t) 2. If both items in (s) are true there is NOFINDING

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

u) If either item in (s) is untrue, this is a FINDING

CCI: CCI-002262

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0730**

Default Severity: Category II

Display User ID Information as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select User Profile, option 1,
- d) Press <ENTER>
- e) On the User Reports screen, select User Summary, option 1,
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Masking Fields area of the screen and enter Y next to the Auditor prompt
- h) Press <ENTER>
- i) On the JCL Submit Processing screen, select S to submit the batch job
- j) Press <ENTER>
- k) Review User Summary report output and ensure that the following items are in effect regarding the AUDITOR attribute:
 1. Authorization to the AUDITOR attribute is restricted to auditing and security personnel.
 2. At minimum, ensure that any users connected to sensitive system dataset HLQ groups or general resource owning groups with the Group-AUDITOR attribute are Auditor and/or Security personnel. Otherwise, Group-AUDITOR is allowed
- l) If both items in (k) are true there is NOFINDING
- m) If either item in (k) is untrue, this is a FINDING

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0740**

Default Severity: Category II

Display FACILITY class Bypass Label Processing (BLP) Information as follows:

- a) From Administrator main menu, select Security Server Reports.
- b) Press <ENTER>
- c) Select General Resource Profile, option 4,
- d) Press <ENTER>
- e) On the General Resource Reports screen, select Access List , option 4,
- f) Tab down to the Batch/Online field, type a B (for batch)
- g) Tab down to the Masking Fields area of the screen and enter ICHBLP by the Profile field and FACILITY by the Class field
- h) Press <ENTER>
- i) On the JCL Submit Processing screen, select S to submit the batch job
- j) Press <ENTER>
- k) If no tape management system (e.g.CA 1) is installed, return to Administrator main menu, select Security Server Commands, option 2, select SETROPTS option 5, locate the CDT Edit prompt on the right hand side of the screen and enter E, press <ENTER>, on the next screen enter L TAPEVOL at the command prompt, when the TAPEVOL information is displayed capture the screen.
- l) Review General Resource Access List report output and ensure the following items are in effect regarding bypass label processing (BLP):
 - 1. The ICHBLP resource is defined to the FACILITY resource class with a UACC(NONE)
 - 2. Access authorization to the ICHBLP resource is restricted at the userid level to data center personnel (e.g. tape librarian, operations staff, etc.)
 - 3. The number of userids authorized to the ICHBLP resource is not excessive.
 - 4. If not tape management system (e.g., CA 1) is installed, the TAPEVOL class is active (as shown on item (v) CDT screen capture)
- m) If all items in (l) are true there is NO FINDING.
- n) If any item in (l) is untrue, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0760**

Default Severity: Category II

Refer to the following items In U_zOS_STIG_INSTRUCTION.doc., Preliminary Worksheet (Part 2 of 2):

- * Item 1
- * Item 13

Display DASDVOL Information as follows:

- a) From Administrator main menu, select Security Server Reports.
 - b) Press <ENTER>
 - c) Select General Resource Profile, option 4,
 - d) Press <ENTER>
 - e) On the General Resource Reports screen, select Access List , option 4,
 - f) Tab down to the Batch/Online field, type a B (for batch)
 - g) Tab down to the Enhanced Masking prompt and enter Y
 - h) Press <ENTER>
 - i) On the Enhanced Masking edit panel, enter the following masking criteria:
CLASS=DASDVOL or CLASS=GDASDVOL
 - j) Press <ENTER>
 - k) On the JCL Submit Processing screen, select S to submit the batch job
 - l) Press <ENTER>
 - m) Review General Resource Access List report output and ensure the following items are in effect regarding DASD volume controls:
 1. A profile of '*' is defined to the DASDVOL resource class.
 2. Access authorization to DASDVOL profiles is restricted to Storage Management Personnel, Storage Management Batch Userids, and Systems Programmers
 3. All profiles defined to the DASDVOL resource class have UACC(NONE).
- NOTE: Volume authorization allows access to all data sets on the volume, regardless of data set profile authorization. Access to operating system and general user storage volumes should be questioned. Refer to Section 3.3.2.5, Special Storage Management Users, and Section 3.3.2.6, Emergency Userids, in the Z/OS STIG for allowable usage of the DASDVOL/GDASDVOL resource classes.***
- n) If all items in (m) are true there is NO FINDING.
 - o) If any item in (m) is untrue, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0770**

Default Severity: Category II

- a) In the Vanguard Administrator go to Option 3;4 which is Security Server Reports; General Resource Profile and then make sure you are in LIVE MODE (type LIVE at the command line). Choose O for ONLINE. In the Standard Masking Fields for CLASS: type in PROGRAM and hit ENTER. On the command line for each profile listed below type LR in the CMD line next to the PROGRAM and PROFILE being checked:
- b) If your Installation DOES NOT use MQSeries, this STEP B can be skipped.
 - 1. Find the following classes in the output and validate that access is restricted per the Auth column in the Sensitive Utility Table in the Stig Addendum.

CSQUTIL
CSQUCVX
CSQJU003
CSQJU004
CSQ1LOGP

- 2. All Access is audited, e.g. ALL(READ)
 - a. If access is granted only as specified in the Sensitive Utility Table and audit is set to ALL(READ) then there is NO FINDING.
 - b. If access is granted to anyone not specified in the Sensitive Utility Table or audit is not set to ALL(READ) then there is A FINDING.
- c) Referring to the Sensitive Utilities Requirements table in the U_zOS_STIG_Addendum, Ensure that all applicable programs or their generic equivalent specified in the table meet the following requirements (e.g. ***GTF**, ***IOCP, *MASPZAP): Type LR next to each and ensure the following:
 - 1. Profile is defined in the PROGRAM resource class.
 - 2. Access is restricted to the appropriate personnel (e.g., systems programming, storage management, etc.) per the Auth column in the Sensitive Utility Table in the Stig Addendum.
 - 3. All access is audited, e.g., ALL(READ).
 - a. If all programs are defined, audited and with appropriate access, then there is NO FINDING
 - b. If any program is not defined, not audited or with inappropriate access, then there is a FINDING

CCI: CCI-000213

CCI: CCI-002234

CCI: CCI-002235

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: RACF0780**

Default Severity: Category II

From a command input screen enter:
RL Global *

Alternately this can be viewed by following steps:
Refer to the following reports produced by the RACF Data
Collection:

- DSMON.RPT(RACGAC)

Examine the Global Access Checking entries.

If Global * is specified in SETROPTS this is a finding.

The following entries may be allowed with the approval of the
ISSM:

Dataset Class - ALTER access level to &RACUID.**

(Allows users all access to their own datasets)

OPERCMDS Class READ access to

MVS.MCSOPER.&RACUID (Allows users access to console
for their jobs)

JESJOBS Class ALTER access to

CANCEL.*.*&RACUID (Allows users to cancel their own
jobs)

JESJOBS Class ALTER access to SUBMIT.*.*&RACUID
(Allows users to submit their own jobs)

The ISSM may allow other classes to be included after evaluation
with the system programmer.

If any other members are included for Global Access Checking this
is a finding.

If written approval by the ISSM is not provided this is a finding.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

Digital Certificates Data Analysis

___STIG ID: ICERR010

Default Severity: Category II

NOTE: The procedures in this checklist item presume the domain being reviewed is running all releases of z/OS, and use the ACP as the certificate store.

The IAO will ensure that for production environments, the list of Certificate Authorities considered trusted by the Z/OS host are limited to those with a trust hierarchy that leads to a DOD PKI Root Certificate Authority.

If the domain being review is not a production system and is only used for test and development, this Self-Signed Certificates review can be skipped.

- a) From STIG ID ITCP0060, use the userid(s) assigned to the TCP/IP address space(s) and issue the following RACF command to list the certificate(s) associated with the TCPIP userid(s):

RACDCERT ID(tcpip userid) LIST

- b) If no certificate information is found, there is NO FINDING.

NOTE: Certificates are only valid when their Status is TRUST. Therefore, you may ignore certificates with the NOTRUST status.

- c) If the digital certificate information indicates that the issuer's distinguished name leads to a DoD PKI Root Certification Authority, External Root Certification Authority (ECA), or an approved External Partner PKI's Root Certification Authority, there is NO FINDING.

Examples of an acceptable DoD CA are:
DoD PKI Class 3 Root CA
DoD PKI Med Root CA

CCI: CCI-002470

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ICERR020**

Default Severity: Category II

NOTE: The procedures in this checklist item presume the domain being reviewed is running all releases of z/OS, and use the ACP as the certificate store.

The IAO will ensure that for production environments, expired certificates are not used.

If the domain being reviewed is not a production system and is only used for test and development, Expired Certificates review can be skipped.

- a) From STIG ID ITCP0060, use the userid(s) assigned to the TCP/IP address space(s) and issue the following RACF command to list the certificate(s) associated with the TCPIP userid(s):

RACDCERT ID(tcpip userid) LIST

- b) If no certificate information is found, there is NO FINDING.

NOTE: Certificates are only valid when their Status is TRUST. Therefore, you may ignore certificates with the NOTRUST status.

- c) Check the expiration for each certificate with a status of TRUST. If the expiration date has passed this is a FINDING.

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ICERR030**

Default Severity: Category II

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

Currently the RACDCERT command does not support a generic userid value of ID(*) LISTMAP to list all the certificate name filters defined to RACF. However, the following commands can be issued to determine if certificate name filtering may be implemented.

- a) If certificate name filtering is in use, collect documentation describing each active filter rule and written approval from the ISSM to use the rule.
- b) Issue the SETROPTS LIST command. If the DIGTNMAP resource class is active, RACF is ready to process any certificate name filters with a Status of TRUST. The DIGTNMAP resource class should not be active unless certificate name filtering is desired.

If the DIGTNMAP resource class is not active, there is NO FINDING.

- c) Certificate name filters are stored as profiles in the DIGTNMAP resource class. The RLIST command is not intended for use with profiles in the DIGTNMAP resource class. However it can be used to determine if any profiles are defined. (NOTE: The information will not be displayed in a suitable format to easily interpret the filter.)

RLIST DIGTNMAP *

If there is nothing to list in the DIGTNMAP resource class, there is NO FINDING.

If profile information is displayed, one or more certificate name filters are defined to RACF. Under the NAME heading of each profile listing is the userid the filter is being mapped to. Issue the following command to list the certificate name filter associated with each userid:

Using Vanguard Administrator's View Digital Mapping Filters option 18;2 with no masking review all Certificate name filters.

NOTE: Certificate name filters are only valid when their Status is TRUST. Therefore, you may ignore filters with the NOTRUST status.

- d) If the DIGTNMAP resource class is active and certificate name filters have a Status of TRUST, certificate name filtering is in use.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- e) If certificate name filtering is in use and filtering rules have been documented and approved by the ISSM, there is NO FINDING.
- f) If certificate name filtering is in use and filtering rules have not been documented and approved by the ISSM, this is a FINDING.

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

CICS Data Analysis

If the installation does not have CICS, the CICS Data Analysis section can be skipped.

Before completing STIGS ZCIC0010- ZCIC0042 please follow these instructions:

Using the CICSSIT JCL in APPENDIX A in the U_zOS_STIG_Instruction.

Copy the JCL to your system and ensure the following items are specified:

- a) CICS load library containing the CICS SIT is specified on the SDFHAUTH DD statement.
- b) Repeat the dump step (i.e., Step 2) for each CICS SIT.
- c) Ensure the PDS member name on the SITDUMP DD statement matches the actual SIT being dumped. This is helpful when matching dumps with specific CICS regions during the data analysis phase.
- d) Add an appropriate jobcard.
- e) Submit CICSSIT for execution. Review the job for error messages to ensure successful execution.
- f) The CICSSIT job will create the partitioned data set:
SYS3.FSO.*xxxx.mmmyyyy*.CICS.RPT - This file will save each SIT dump in individual members. This data set and its members will be referenced in the CICS Data Analysis.

Collect data using the on-line ISPF facilities.

1. Create a list of sensitive CICS datasets as the basis for subsequent analysis.
 - a) Allocate a partitioned dataset with LRECL(80), named **'sys3.fso.*xxxx.mmmyyyy*.dsnlist'** to which a member can be added for each of the products to be analyzed. The respective members will contain the names of all of the infrastructure datasets related to that software product.
 - b) Review the members for each of the CICS PROCs in the **'sys3.fso.*xxxx.mmmyyyy*.cicsproc'** dataset to identify the CICS infrastructure dataset naming convention and the names of individual CICS datasets.
CICS infrastructure data set names are identified by DD names beginning with **DFH**. Also include any dataset name allocated by the **SYSIN** DD statement containing CICS system initialization parameters.
Based on the naming convention in use, use ISPF/PDF option 3.4 data

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

set name list (e.g., ****.*CICS***) to obtain a comprehensive list of CICS product data sets, including installation data sets not referenced in PROCLIB members

- c) Create a member in the DSNLIST dataset named 'CICSDSNS'. Include all of the CICS infrastructure dataset names identified in step b) above. Enter each dataset name in the member on its own line and starting in column 1

This list of dataset names displayed using ISPF/PDF option 3.4 can generally be copied using "copy and paste" into the CICSDSNS member of the DSNLIST dataset. Any additional CICS dataset names identified in the CICSPROC dataset that do not follow the typical naming convention can then be added.

Note: There may well be datasets specified in the CICS PROC JCL that are related to other software such as Omegamon for CICS for which it may be appropriate to create a separate member in the DSNLIST dataset.

2. Collect CICS PROCLIB member lists and JC.

- a) Identify the system PROCLIB containing the JES2 PROC by referring to the MSTJCLxx member in PARMLIB. The JES2 PROC in use will be the first instance of a JES2 PROC in the dataset concatenation associated with the IEFPSI DD statement.
- b) In the JES2 PROC identify the PROCLIB datasets identified by the PROC00 DD statement.
- c) Identify any dynamic PROCLIB datasets by issuing the system command:
/SD PROCLIB
A response of "NO SELECTABLE ENTRIES FOUND MATCHING SPECIFICATION" indicates that no dynamic PROCLIB datasets are in use.
- d) Use the ISPF Search-For Utility (ISPF 3.14) to identify any procedures used to initiate CICS execution by specifying DFHSIP as the SEARCH STRING.

- 1. The search must be conducted for each of the PROCLIB datasets identified in Steps 2 and 3 above. The search can be performed in batch as a single job with

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

all of the PROCLIB datasets concatenated on the NEWDD DD statement in the same sequence that they appear on the PROC00 DD statement in the JES2 PROC.

2. The output from the ISRSUPC program can be directed to a sequential dataset named: '**sys3.fso.xxxx.mmmyyyy.cicsproc.names**' or be allowed to be directed to SYSOUT by default.
3. Allocate a partitioned dataset named: '**sys3.fso.xxxx.mmmyyyy.cicsproc**' to which each of the CICS PROCs identified in Step 6 can be copied for further analysis.
4. Copy each of the CICS PROCs identified in Step 6 to the '**sys3.fso.xxxx.mmmyyyy.cicsproc**' dataset for use during subsequent CICS analysis STIGs.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCIC0010**

Default Severity: Category II

- a) From the Analyzer Main Menu
 - 1. Enter Option '4;B' and press <ENTER>
 - 2. On the "Sensitive and Critical Data Sets Analysis" panel, place an 'R,' preceding "User defined list".
 - 3. Key in the name of the dataset and member that contains the list of all of the CICS infrastructure dataset names, for which the suggested name is:

'sys3.fso.xxxx.mmmyyyy.dsnlist(cicsdsns)

in the "Fully qualified (without quotes) name of data set containing list:" field.
 - 4. Specify 'NO' for the "RACF Group Detail", "Sort Criteria" and "Exceptions Only" options.
 - 5. Press <ENTER>
 - 6. On the "JCL Submit Processing" panel specify Option 'E' to edit the generated JCL and press <ENTER>
 - 7. On the subsequent ISPF EDIT panel modify the REPORT DD statement in the Analyzer batch JCL to specify the dataset to which the Analyzer Sensitive Data Sets Report should be written. If DCB parameters are specified, the data set must be allocated with RECFM(FBA) and LRECL(133) attributes. Alternatively, you may wish to pre-allocate a PDS or PDSE with RECFM(FBA) and LRECL(133) attributes, such that individual Analyzer Reports can be created as individual members in a single dataset..
 - 8. After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering 'submit' on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing" panel and then specify Option 'S' to submit the Administrator Job for execution.
- b) Review the VSA report output for each data set analyzed.

UPDATE and/or ALTER access to CICS system datasets is restricted to systems programming personnel.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

Note: The CICS region userids, the userids under which the CICS started Tasks execute, will also need UPDATE to many of the CICS infrastructure datasets and will need CONTROL access to CICS datasets for which the lowest level dataset name qualifier is typically DFHINTRA and DFHTEMP.

- c) If (b) is true, there is NO FINDING.
- d) If (b) is untrue, this is a FINDING.

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCIC0020**

Default Severity: Category II

- a) From Administrator Main Menu, enter Option '3;4' and press <ENTER>
- b) On the "General Resource Reports" panel specify Option '4' on the "COMMAND" line to request an "Access Lists" report.

Specify 'B' for the "Batch/On-line:" Option.

Specify the RACF member class name used to control access to CICS transactions, (e.g. TCICSTRN) for the CLASS: Masking Criteria.

Press <ENTER>

- c) On the "Processing Options" panel specify 'Y' for "Explode RACF groups in access lists at end of report"

Press <ENTER>

- d) On the "JCL Submit Processing" panel specify Option 'E' to edit the generated JCL and press <ENTER>.
- e) On the subsequent ISPF EDIT panel modify the PRNT DD statement in the Administrator batch JCL to specify the dataset to which the Access Lists report should be written. If DCB parameters are specified the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.
- f) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering 'submit' on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing" panel and then specify Option 'S' to submit the Administrator Job for execution.
- g) Return to the "General Resource Reports" panel by pressing <PF3> a sufficient number of time and then repeat steps b) through f) for the RACF group class name used to control access to CICS transactions.

If installation defined classes are used to control access to CICS transaction, then these steps, b) through f), must be repeated for each member and group class in use.

Alternatively, you may wish to produce Access List Reports for all of the member and group classes used for CICS transaction security in a single Administrator Job, with the reports written successively to a single dataset.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

This can be accomplished when editing the generated JCL in step b) by replicating the four Administrator control statements, beginning with the REPORT statement and ending with the REPORT(END) statement, for each member and group resource class to be reported. The CLASS(name) statement must be changed within each set of four control statements to specify the desired resource class name.

Note: If the series of reports to be produced are to be directed to a dataset, ensure that DISP=(MOD,CATLG) has been specified in the PRNT DD statement. As the output dataset is closed in response to each REPORT(END) statement encountered, failure to do so will cause each report produced to overlay the preceding report.

- h) Ensure the following items are in effect for *all* CICS regions:

Refer to the information gathered from the CICS Systems Programmer s Worksheet in the Preliminary Information Worksheets in U_zOS_STIG_INSTRUCTION.doc.

1. Transactions listed in tables CICS CATEGORY 2 CICS AND OTHER PRODUCT TRANSACTIONS and CICS CATEGORY 4 COTS-SUPPLIED SENSITIVE TRANSACTIONS, in the z/OS STIG Addendum, are restricted to authorized personnel.

Note: The exception to this is the CEOT and CSGM transactions, which can be made available to all users.

Note: The transactions beginning with "CK" apply to regions running WebSphere MQ.

Note: Category 1 transactions are internally restricted to CICS region userids.

2. If the domain being reviewed is running MQSeries/WebSphere MQ, transactions listed in Section 4.3.4.2.11, CICS Transaction Security in the Z/OS STIG are restricted to CICS region userids, system programming personnel, and MQSeries administrators.

- i) If the items mentioned in (h) are true for all CICS transaction resource classes,, there is NO FINDING.
- j) If any item mentioned in (h) is untrue for a CICS transaction resource class, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCICR021**

Default Severity: Category II

- a) From the Analyzer Main Menu, enter Option '4;1' and press <ENTER>
- b) On the "RACF Class Descriptor Table Analysis" panel, press <ENTER>.
- c) On the "JCL Submit Processing" panel specify Option 'E' to edit the generated JCL and press <ENTER>
- d) On the subsequent ISPF EDIT panel modify the REPORT DD statement in the Analyzer batch JCL to specify the dataset to which the Analyzer RACF Class Descriptor Table Analysis Report should be written. If DCB parameters are specified, the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.

Alternatively, you may wish to pre-allocate a PDS or PDSE with RECFM(FBA) and LRECL(133) attributes, such that individual Analyzer Reports can be created as individual members in a single dataset.

- e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering 'submit' on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing" panel and then specify Option 'S' to submit the Administrator Job for execution.

<ENTER>

- f) Refer to the information gathered from the CICS Systems Programmer's Worksheet in the Preliminary Information Worksheets (Appendix B).
- g) Ensure each CICS transaction resource class pair is active.
- h) If (g) is true for all CICS recourse classes, there is NO FINDING.
- i) If (g) is untrue for any CICS recourse class, there is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCIC0030**

Default Severity: Category II

1. Gather from your CICS programmer the list of JCL used to start each CICS region. Generally these will be found in a proclib member.

Refer to the information gathered from the CICS Systems Programmers Worksheet in the Preliminary Information Worksheets.

Refer to the CICS region SYSLOG - (Alternate source of SIT parameters). Be sure to process DFHSIT based on the order specified in Note 2 Refer to the CICS

2. Ensure the following CICS System Initialization Table (SIT) parameter settings are specified for *each* CICS region:

(NOTE: CICS system initialization parameters are specified in the following ways:

- In the system initialization table, loaded from a library in the STEPLIB concatenation of the CICS startup procedure.
- In the PARM parameter of the EXEC PGM=DFHSIP statement of the CICS startup procedure.
- In the SYSIN data set defined in the startup procedure (but only if SYSIN is coded in the PARM parameter).

The system initialization parameters are processed in the preceding order, with later system initialization parameter values overriding those specified earlier).

1. SEC=YES

If **SEC** is not coded in the CICS region startup JCL, go to offset x'117' from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the external security setting in bold:

**X'80' EQU B'10000000' EXTERNAL SECURITY
REQUESTED**

X'40' EQU B'01000000' RESOURCE PREFIX REQUIRED
X'10' EQU B'00010000' RACLIST class APPCLU required

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

X'08' EQU B'00001000' ESM INSTLN data is required
X'04' EQU B'00000100' Surrogate User Checking required
X'02' EQU B'00000010' Always enact resource check
X'01' EQU B'00000001' Always enact command check

2. **DFLTUSER=CICSUSER** | userid

If **DFLTUSER** is not coded in the CICS region startup JCL, go to offset x'118' from the beginning on the SIT dump (record sequence number – 6) for a length of 8 bytes. The value will be the CICS default userid.

3. **XUSER=YES**

If **XUSER** is not coded in the CICS region startup JCL, go to offset x'117' from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the surrogate user checking setting in bold:

X'80' EQU B'10000000' EXTERNAL SECURITY
REQUESTED
X'40' EQU B'01000000' RESOURCE PREFIX REQUIRED
X'10' EQU B'00010000' RACLIST class APPCLU required
X'08' EQU B'00001000' ESM INSTLN data is required
X'04' EQU B'00000100' Surrogate User Checking required
X'02' EQU B'00000010' Always enact resource check
X'01' EQU B'00000001' Always enact command check

4. **SNSCOPE=NONE** | CICS | MVSIMAGE | SYSPLEX

If **SNSCOPE** is not coded in the CICS region startup JCL, go to offset x'124' from the start of the SIT dump (record sequence number - 6) for a length of 1. This is the signon scope byte flag. Below are the possible hex settings for this flag:

X'01' EQU 1 SIGNON SCOPE = NONE
X'02' EQU 2 SIGNON SCOPE = CICS
X'03' EQU 3 SIGNON SCOPE = MVSIMAGE
X'04' EQU 4 SIGNON SCOPE = SYSPLEX

NOTE: **SNSCOPE=NONE** is *only* allowed with test/development regions.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

For SNSCOPE value check the following:

- a. If there is one production CICS region then SNSCOPE must be set to 'CICS', so that a particular userid cannot be logged on multiple times within the same region.
(If this parameter is not specified in the CICS startup JCL verify that its value is x'02' at offset x124 in the SIT).
- b. If there are multiple CICS regions within the scope of one MVS image then SNSCOPE must be set to 'MVSIMAGE', so that a particular userid cannot be logged on more than once within the scope of one MVSIMAGE.
Also every CICS region in the MVSIMAGE must have the value 'MVSIMAGE' specified for SNSCOPE.
(If this parameter is not specified in the CICS startup JCL, verify that its value is x'03' at offset x'124' in the SIT).
- c. If there are multiple CICS regions within the scope of one SYSPLEX then SNSCOPE must be set to 'SYSPLEX' so that a particular userid cannot be logged on multiple times within the scope of one SYSPLEX. Also every CICS region in the SYSPLEX must have this same value, specified for SNSCOPE.
If this parameter is not specified in the CICS startup JCL, then verify that its value is x'04' at offset x'124' in the SIT).

5. XTRAN=YES | ssrrTRN | classname

If **XTRAN** is not coded in the CICS region startup JCL, go to offset x'CA' from the beginning on the SIT dump (record sequence number - 6) for a length of 7 bytes. The value will be the resource class name used for that region. If **XTRAN=YES** is coded, c'CICSTRN' will be present.

6. SECPRFX=YES

If **SECPRFX** is not coded in the CICS region startup JCL, go to offset x'117' from the beginning on the SIT dump (record sequence number - 6) for a length of 1. This is the security byte flag. Below are the hex and bit settings for this flag with the resource prefixing setting in bold:

X'80' EQU B'10000000' EXTERNAL SECURITY REQUESTED
X'40' EQU B'01000000' RESOURCE PREFIX REQUIRED
X'10' EQU B'00010000' RACLIST class APPCLU required
X'08' EQU B'00001000' ESM INSTLN data is required
X'04' EQU B'00000100' Surrogate User Checking required

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

X'02' EQU B'00000010' Always enact resource check
X'01' EQU B'00000001' Always enact command check

***NOTE 1:** If **XTRAN=ssrrTRN** is specified, resource prefixing (e.g. **SECPRFX=YES**) is **not** required to be enabled. Also, CICS regions cannot share the same resource class if resource prefixing is not active.*

- b) If the SIT parameters are defined as specified in (b) for each CICS region, there is NO FINDING.
- c) If any SIT parameter is not defined as specified in (b) for a CICS region, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCIC0040**

Default Severity: Category II

- a) From the Analyzer Main Menu, enter Option '4;4' and press <ENTER>
- b) On the "RACF Started Procedure Table Analysis" panel, press <ENTER>.
- c) On the "JCL Submit Processing" panel specify Option 'E' to edit the generated JCL and press <ENTER>
- d) On the subsequent ISPF EDIT panel modify the REPORT DD statement in the Analyzer batch JCL to specify the dataset to which the Analyzer RACF Started Procedure Table Analysis Report should be written. If DCB parameters are specified, the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.

Alternatively, you may wish to pre-allocate a PDS or PDSE with RECFM(FBA) and LRECL(133) attributes, such that individual Analyzer Reports can be created as individual members in a single dataset.

- e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering 'submit' on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing" panel and then specify Option 'S' to submit the Administrator Job for execution.

<ENTER>

- f) Refer to the information gathered by the Z/OS & z/OS Data Collection in the following dataset:

- **sys3.fso.xxxx.mmmyyyy.cicsproc**

Refer to the information gathered from the CICS Systems Programmer's Worksheet in the Preliminary Information Worksheets (Appendix B).

- g) Ensure that the following is defined for each CICS region:
 - 1. A unique userid is defined.
 - 2. The Procedure is defined to the STARTED resource class with attributes of PRIVILEGED(NO) and TRUSTED(NO).

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- h) If (g) is true for all CICS regions, there is NO FINDING.
- i) If (g) is untrue for any CICS region, there is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCIC0041**

Default Severity: Category II

- a) From Administrator Main Menu, enter Option '11;4' and press <ENTER>
- b) On the "Data Services" panel specify Option '4' on the "COMMAND" line to request an "Tailor Administrator Batch JCL" and press <ENTER>.
- c) On the "Batch Execution Job Statement" panel supply an appropriate JOB statement for executing batch jobs and press <ENTER>
- d) On the "Administrator Batch Environment" panel supply:
 - in response to the "ADMINISTRATOR JCL DSN" the name of a PDS to which the customized JCL for the Administrator batch jobs should be written,
 - in response to the "Batch Command DSN" the name of a sequential dataset that will be created during the execution of the Administrator batch jobs to contain the RACF commands generated by the batch job,and press <ENTER>
- e) Display the dataset specified as the "ADMINISTRATOR JCL DSN" in the preceding Step using ISPF/PDF option 3.4 data set name list and edit the member named VRARBLDJ containing JCL for the Administrator Batch REBUILD Facility.

Following the "//STEP02.SYSIN DD *" DD statement, replace the sample "COMMAND(REBUILD GROUP) *" statement with a "COMMAND(REBUILD USER) *" statement. Following this statement remove the sample group name of SYS1 and include a line containing each userid, beginning in column 1, used as the CICS default user for any of the CICS regions.

Save these changes and submit the VRARBLDJ Job for execution.

- f) View the generated REBUILD commands for each of the CICS default user userids to ensure the following items are in effect :
 - 2. The userid has not been granted the RACF **OPERATIONS** attribute.
 - 3. No access to interactive on-line facilities (e.g., TSO) other than CICS.
 - 4. A CICS segment has been defined and the **TIMEOUT** parameter is set to 15 minutes.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

5. The userid is restricted from accessing all data sets and resources with the following exceptions:
 6. Non-restricted CICS transactions (e.g., CESF, CESN, 'good morning' transaction, etc.)
 7. If applicable, resources necessary to operate in an intersystem communication (ISC) environment (i.e., LU6.1, LU6.2), and/or CICS multi-region environment (MRO)
 - g) If (f) is true for all CICS default userids, there is NO FINDING
 - h) If (f) is untrue for any CICS default userid, there is a FINDING.
 - i) NOTE: A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain the documentation for each system with a time-out adjusted beyond the 15-minute recommendation to explain the basis for this decision

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZCICR041**

Default Severity: Category II

- a) From Administrator Main Menu, enter Option '3;4' and press <ENTER>
- b) On the "General Resource Reports" panel specify Option '1' on the "COMMAND" line to request a "General Resource Profile Summary" report.

Specify 'B' for the "Batch/On-line:" Option.

Specify the PROPCNTL class name for the CLASS: Masking Criteria.

Press <ENTER>

Note: Administrator may have to be in 'Extract' mode in order for the batch option to work. If it does not allow a batch transaction, put 'EXTRACT' in the command line and <ENTER>. Then enter in the data from step b again.

- c) On the "JCL Submit Processing" panel specify Option 'E' to edit the generated JCL and press <ENTER>.
- d) On the subsequent ISPF EDIT panel modify the PRNT DD statement in the Administrator batch JCL to specify the dataset to which the Access Lists report should be written. If DCB parameters are specified the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.
- e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering 'submit' on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing" panel and then specify Option 'S' to submit the Administrator Job for execution.
- f) Compare the results from the generated report to the data gathered from the CICS Systems Programmer's Worksheet in the Preliminary Information Worksheets, Appendix B.
- g) Check that each CICS region userid is defined as a profile name in the **PROPCNTL** resource class
- h) If (g) is true for every CICS region userid, there is NO FINDING,
- i) If (g) is untrue for any CICS region userid, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZCIC0042**

Default Severity: Category II

- a) From Administrator Main Menu, enter Option '3;5' and press <ENTER>
- b) On the "Profile Segment Reports" panel specify Option '3' on the "COMMAND" line to request a "CICS User Segment" report.

Specify 'B' for the "Batch/On-line:" Option (make sure Data is on Extract, not live, mode).

Press <ENTER>

- c) On the "JCL Submit Processing" panel specify Option 'E' to edit the generated JCL and press <ENTER>.
- d) On the subsequent ISPF EDIT panel modify the PRNT DD statement in the Administrator batch JCL to specify the dataset to which the Access Lists report should be written. If DCB parameters are specified the data set must be allocated with RECFM(FBA) and LRECL(133) attributes.
- e) After making any desired changes to the generated JCL, submit the Administrator Job for execution either by entering 'submit' on the command line of the ISPF EDIT panel or press <PF3> to return to the JCL Submit Processing" panel and then specify Option 'S' to submit the Administrator Job for execution.
- f) Ensure that all userids with a CICS segment have the **TIMEOUT** parameter set to **15** minutes.
- g) If (f) is true for each CICS user, there is NO FINDING.

***NOTE:** If the time-out limit is greater than 15 minutes, **and** the system is processing unclassified information, review the following items. If any of these is true, there is NO FINDING.*

- h) If a session is not terminated, but instead is locked out after 15 minutes of inactivity, a process must be in place that requires user identification and authentication before the session is unlocked. Session lock-out will be implemented through system controls or terminal screen protection.
- i) A system's default time for terminal lock-out or session termination may be lengthened to 30 minutes at the discretion of the IAM. The IAM will maintain the documentation for each system with a time-out adjusted

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

beyond the 15-minute recommendation to explain the basis for this decision.

- j) The IAM may set selected userids to have a time-out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception must meet the following criteria:
- k) The time-out exception cannot exceed 60 minutes.
- l) A letter of justification fully documenting the user requirement(s) must be submitted and approved by the site IAM. In addition, this letter must identify an alternate means of access control for the terminal(s) involved (e.g., a room that is locked at all times, a room with a cipher lock to limit access, a password protected screen saver set to 30 minutes or less, etc.).
- m) The requirement must be revalidated on an annual basis.
- n) If the CICS time-out limit is not specified for 15 minutes of inactivity, and the previously mentioned exceptions do not apply, this is a FINDING.

CCI: CCI-000057

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

FEP Data Analysis

___**STIG ID: ZFEP0011**

Default Severity: Category II

- a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 1, in the Preliminary Information Worksheets (Appendix B):
 - Item 1: Documents and procedures restricting access to the hardware components of the FEPs.
- b) If the hardware components of the FEPs are located in secure locations, there is NO FINDING.
- c) If the hardware components of the FEPs are not located in secure locations, this is a FINDING.

CCI: CCI-000933

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZFEP0012**

Default Severity: Category II

- a) Refer to the Front End Processor (FEP) Protection Worksheet, Items 1-4, in the Preliminary Information Worksheets (Appendix B):
- Item 1: Documents and procedures restricting access to the hardware components of the FEPs.
 - Item 2: Documents and procedures restricting access to the functions of the service subsystem from the control panel.
 - Item 3: Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).
 - Item 4: Documents and procedures restricting access to the diskette drive of the service subsystem.
- b) If a procedure is in place to restrict access to the functions of the service subsystem, there is NO FINDING.
- c) If a procedure is in place to restrict access to the functions of the service subsystem from operator consoles (local and/or remote), there is NO FINDING.
- d) If a procedure is in place to restrict access to the diskette drive of the service subsystem, there is NO FINDING.
- e) If no procedure exists for any of the above functions of the service subsystem and FEP resources, this is a FINDING.

CCI: CCI-000004

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZFEP0013**

Default Severity: Category II

- a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 6, in the Preliminary Information Worksheets (Appendix B):
 - Item 6: Documents and procedures regarding the **NCP** load and dump processes.
- b) If a procedure is in place relative to the **NCP** load and dump processes, there is **NO FINDING**.
- c) If no procedure is in place relative to the **NCP** load and dump processes, this is a **FINDING**.

CCI: CCI-000504

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZFEP0014**

Default Severity: Category II

- a) Refer to the Front End Processor (FEP) Protection Worksheet, Item 8, in the Preliminary Information Worksheets (Appendix B):
 - Item 8: All documents and procedures that apply to FEP operations including network management, FEP initialization, IPL, shutdown, **NCP** dumping, backup, and recovery.
- b) If a log is in place to keep track of all hardware upgrades and software changes, there is NO FINDING..
- c) If a log is in place to keep track of all hardware upgrades and software changes, there is NO FINDING.

CCI: CCI-000318

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZFEP0015**

Default Severity: Category II

- a) Reference data from item 4 of the Z/OS Systems Programmer's Worksheet, located in Appendix B to locate the JES2 proclibs.
- b) Search the JES2 proclibs for the member that executes program ISTINM01. These data sets are used for the FEP at the site; if the domain does not have a FEP the collection of these data sets can be bypassed. Review the VTAM procedure for load and dump data sets for the FEP. Use ISPF/PDF option 3.4 data set name list to enter ****.*NCP***. Enter the names of the above datasets in a sequential dataset. Make note of the dataset name for item C below.
- c) From Analyzer main Menu, go to B, "Sensitive Critical Data Sets Analysis", enter "R" to the left of "User defined list". Enter the name of the sequential dataset created from above to the right of the **=>**. Press enter.
- d) Review the "User defined list" shown. If there are entries in the displayed list that have either R, N, E, or W in the "M" column, there is a FINDING for NCP data sets allowing inappropriate access.
- e) Review each data set shown in the "User defined list" by entering "VRC" under the "Opt" heading. Check the access to these data set rules to ensure they do not allow UPDATE and/or ALTER access to authorized personnel (e.g., Z/OS systems programming personnel). If any allow UPDATE or ALTER access, this is a FINDING

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZFEP0016**

Default Severity: Category II

- a) Refer to the Front End Processor (FEP) Protection Worksheet, Items 1-4, in the Preliminary Information Worksheets (Appendix B):
- Item 1: Documents and procedures restricting access to the hardware components of the FEPs.
 - Item 2: Documents and procedures restricting access to the functions of the service subsystem from the control panel.
 - Item 3: Documents and procedures restricting access to the functions of the service subsystem from the local and/or remote operator consoles (e.g., physical access, password control, key-lock switch of modems, etc.).
 - Item 4: Documents and procedures restricting access to the diskette drive of the service subsystem.
- b) If a password control is in place to restrict access to the service subsystem via the operator consoles (local and/or remote), there is NO FINDING.
- a) If a key-lock switch is used to protect the modem supporting the remote console of the service subsystem, there is NO FINDING.
- b) If no procedure exists for any of the above functions of the service subsystem and FEP resources, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

IBM Communications Server Data Analysis

___STIG ID: IFTP0010

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the FTP daemon runs under its own user account. Specifically, it does not share the account defined for the Z/OS UNIX kernel.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the FTP daemon.

Find the FTPD USERID. Document the FTPD ID: _____

- b) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the OMVS daemon.

Find the OMVS USERID. The OMVS USER ID is _____

- c) Review Vanguard Analyzer RACF Started Procedures Table Analysis option 3; 4

- d) There is an entry in the STARTED resources class for FTP daemons _____ True
_____ False

- e) All of FTPD(s) USERID are FTPD _____ True _____ False

- f) The FTPD(S) USERID is not the same as OMVS USERID _____ True
_____ False

- g) The FTPD(s) USERIDs are defined as a PROTECTED _____ True _____
False_____

- h) Review the FTP USERID with Vanguard Administrator User Reports option 3; 1 Mask on USERID=USERID documented above

1. Type LV on CMD space next to USER ID

2. Insure FTPD(s) userid has the following OMVS Segments attributes:

The UID value is 0 _____ True _____ False

There is a HOME directory / _____ True _____ False

There is a shell program defined /bin/sh _____ True _____ False

- i) If any items above are False this is a FINDING for STIG ID IPFTP0010

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0020**

Default Severity: Category II

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

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member. **NOTE: The JCL member is typically named FTPD.**

Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started tasks.

- b) Review the FTP daemon's started task JCL:
 - 1. The SYSTCPD and SYSFTPD DD statements specify the TCP/IP Data and FTP Data configuration files respectively. ____ True ____ False
 - 2. The ANONYMOUS keyword is not coded on the PARM parameter on the EXEC statement. ____ True ____ False
 - 3. The ANONYMOUS=logonid combination is not coded on the PARM parameter on the EXEC statement. ____ True ____ False
 - 4. The INACTIVE keyword is not coded on the PARM parameter on the EXEC statement. ____ True ____ FALSE

The AUTOLOG statement block can be configured to have TCP/IP start the FTP Server. The FTP entry (e.g., FTPD) can include the PARMSTRING parameter to pass parameters to the FTP procedure when started. NOTE: Parameters passed on the PARMSTRING parameter override parameters specified in the FTP procedure

- c) Review the AUTOLOG statement block with in the PROFILE DD of the each TCPIP started task JCL. If an FTP entry is configured in the AUTOLOG statement block in the TCP/IP Profile configuration file, ensure the following items are in effect:
 - 1. The ANONYMOUS keyword is **not** coded on the PARMSTRING parameter.
 - 2. The ANONYMOUS=logonid combination is **not** coded on the PARMSTRING parameter.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

3. The INACTIVE keyword is **not** coded on PARMSTRING parameter.
- d) If any items above are False this is a FINDING for STIG ID IFTPP020

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0030**

Default Severity: Category II

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 OS390 STIG Volume 1 Table 4.4.41.3.a

FTP.DATA CONFIGURATION STATEMENTS

ANONYMOUS_	[Not Coded]
BANNER	[An HFS file, e.g., /etc/ftp.banner]
INACTIVE_	[A value between 1 and 900]
UMASK_	077

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the FTP daemon.

If FTP is inactive, review the procedure libraries defined to JES2 and locate the FTP JCL member. **NOTE: the JCL member is typically named FTPD.**

- b) Locate the SYSFTPD statement in all active FTPD started tasks JCL members executing on the domain.
- c) From the ISPF Primary Option Menu use option 3.4 and review the FTP daemon's started task configuration identified by the SYSFTPD statement. Ensure the following items are in effect for the configuration statements specified in the FTP Data configuration file:
 - a) The **ANONYMOUS** statement is not coded (does not exist) or, if it does exist, it is commented out. ____ True ____ False

NOTE: Other statements prefixed with ANONYMOUS may be present. These statements indicate the level of anonymous support and applicable restrictions if anonymous support is enabled using the ANONYMOUS statement. These other ANONYMOUS-prefixed statements may be ignored.

- b) The **INACTIVE** statement is coded with a value between 1 and 900 (seconds). ____ True ____ False

NOTES: 900 indicates a session timeout value of 15 minutes.
0 disables the inactivity timer check.

- c) The **UMASK** statement is coded with a value of 077. ____ True ____ False
- d) The **BANNER** statement is coded. ____ True ____ FALSE

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

d) If any items above are False this is a FINDING for STIG ID IPFTP030

CCI: CCI-000048

CCI: CCI-000366

CCI: CCI-001133

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0040**

Default Severity: Category II

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

- a) Refer to the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL. From the ISPF Primary Option Menu use option 3.4 and review the file(s) allocated by the STEPLIB DD statement in the FTP started task JCL.
 - 1. Refer to the libraries specified in the system Linklist and LPA.
 - 2. Refer to APPENDIX B for the information gathered from the IBM Communications Server Worksheet in the Preliminary Information Worksheets.

b) Ensure the following items are in effect for FTP Server user exits: The FTCHKCMD, FTCHKIP, FTCHKJES, FTCHKPWD, FTPOSTPR, and FTPSMFEX modules are not located in the FTP daemon's STEPLIB, Linklist, or LPA.

NOTE: The ISPF ISRFIND utility can be used to search the system Linklist and LPA for specific modules.

Ensure that SMFEXIT= is not specified in the FTP DATA configuration file enabling the FTPSMFEX exit.

- c) If both of the above are true, there is NO FINDING.
- d) If any FTP Server user exits are implemented and the site has written approval from DISA FSO to install and use the exits, there is NO FINDING.
- e) If any FTP Server user exits are implemented and the site has not obtained written approval from FSO to install and use the exits, this is a FINDING.

CCI: CCI-000382

CCI: CCI-001764

CCI: CCI-001765

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0050**

Default Severity: Category II

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

- a) From the ISPF Primary Option Menu use option 3.4 and review the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.
- b) Ensure the BANNER statement in the FTP Data configuration file specifies an HFS file or data set that contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys,

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: IFTP0060

Default Severity: Category II

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

- a) From the ISPF Primary Option Menu use option 3.4 and review the Data configuration file specified on the SYSFTPD DD statement in the FTP started task JCL.
- b) Ensure the following items are in effect for the configuration statements specified in the FTP Data configuration file:
 - 1. The SMF statement is coded with a value of TYPE119.
 - 2. The SMFJES and SMFSQL are coded with value of TYPE119
 - 3. The SMFAPPE, SMFDEL, SMFEXIT, SMFLOGN, SMFREN, SMFRETR, and SMFSTOR statements are not coded or commented out.
- c) If all of the above are true, there is NO FINDING.
- d) If any of the above is untrue, this is a FINDING.

CCI: CCI-000130

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0070**

Default Severity: Category II

The systems programmer responsible for supporting ICS will 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 FTP SERVER HFS OBJECT SECURITY SETTINGS (4.4.4.2 a)

- a) Using Vanguard Administrator UNIX file manager option 14 review the files listed below.
- b) If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the list below, there is NO FINDING.

HFS file name	Permission Bits	User Audit bits
/usr/sbin/ftpd	1740	fff
/usr/sbin/ftpdns	1755	fff
/usr/sbin/tftpd	0644	faf
/etc/ftp.data	0744	faf
/etc/ftp.banner	0744	faf

NOTES: Some of the files listed above are not used in every configuration. Absence of a file will not be considered a FINDING.

- 1. 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 must have the required settings.
- 2. The /etc/ftp.data file may not be the configuration file the server uses. It is necessary to check the SYSFTPD DD statement in the FTP started task JCL to determine the actual file.
- 3. The /etc/ftp.banner file may not be the banner file the server uses. It is necessary to check the BANNER statement in the FTP Data configuration file to determine the actual file. Also, the permission bit setting for this file must be set as indicated in the table above. A more restrictive set of permissions is not permitted.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx(least restrictive)
6 rw-
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
-no auditing

c) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: IFTP0080

Default Severity: Category II

The IAO will ensure that if present, the data set containing the FTP.DATA configuration file allows read access to all authenticated users and all other access is restricted to systems programming personnel. The IAO will ensure that all write and allocate access to the data set containing the FTP.DATA configuration file is logged. The IAO will ensure that if present, the data set containing the FTP banner file allows read access to all

- a) Locate the SYSFTPD statement in all active FTPD started tasks JCL members executing on the domain..
- b) Using Vanguard Administrator Ensure the following data set controls are in effect for the FTP Server:
 1. Using On-line Access and Authorization option 4 review the profile protecting the dataset identified in (A) UPDATE and ALTER access to the data set containing the FTP Data configuration file is restricted to systems programming personnel.
Document the protecting profile(s)

NOTE: READ access to all authenticated users is permitted.

2. Using AUDIT FLAGS option 3;3;2 review all profiles identified in (1) to ensure UPDATE and ALTER access to the data set containing the FTP Data configuration file is logged.
3. From the ISPF Primary Option Menu use option 3.4 and review the banner statement located in the FTP configuration file. Using On-line Access and Authorization option 4 review the profile protecting the dataset identified to ensure UPDATE and ALTER access to the data set containing the FTP banner file is restricted to systems programming personnel.
4. From the ISPF Primary Option Menu use option 3.4 and review the banner statement located in the FTP configuration file. Using AUDIT FLAGS option 3;3;2 review all profiles identified in (1) READ access to the data set containing the FTP banner file is permitted to all authenticated users.

NOTES:

The MVS data sets mentioned above are not used in every configuration.
Absence of a data set will not be considered a FINDING.

The data set containing the FTP Data configuration file is determined by checking the SYSFTPD DD statement in the FTP started task JCL.

The data set containing the FTP banner file is determined by checking the BANNER statement in the FTP Data configuration file.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0090**

Default Severity: Category II

The IAO will ensure that Userid and password is coded on separate statements to prevent the display of the password in the output file.

- a) Using Vanguard Administrator General Resource report option 3.4 Mask on class=program
- b) Ensure the following program controls are in effect for the TFTP Server:
 - 1. Program resources TFTPDP and EZATD are defined to the PROGRAM resource class with a UACC(NONE). The library name where these programs are located is hlq.TCPIP.SEZALOAD.
 - 2. No access to the program resources TFTPDP and EZATD is permitted.
- c) If both the items in (b) are true, there is NO FINDING.
- d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-001764

CCI: CCI-002235

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0100**

Default Severity: Category II

The IAO will ensure that For batch jobs, the INPUT DD statement does not refer to in-stream data (i.e., "DD *") if that data contains a password.

- a) Refer to APPENDIX B for the following items gathered from the File Transfer Protocol (FTP) Worksheet in the Preliminary Information Worksheets:
 - 1. Item 5 (List of all FTP userids defined to the ACP database, including the function and purpose of each FTP userid.)
- b) Ensure that an Acknowledgement of Risk Letter exist for all userids utilizing unencrypted communications.
- c) If (b) is true, there is NO FINDING.
- d) If (b) is untrue, this is a FINDING

CCI: CCI-000041

CCI: CCI-000042

CCI: CCI-001037

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IFTP0110**

Default Severity: Category II

- a). Verify that FTP login information (USER IDS and Passwords for connecting to remote systems) is not kept in unprotected data sets, in-stream JCL etc. If they are, this is a FINDING.
- b) Consult with the operations personnel/systems programmers in your organization to identify the names of the datasets that contain the FTP USER IDs and PASSWORDs for logging into /connecting to, other systems
- c) Ensure the following data set controls are in effect for the data sets containing FTP login information (USER IDs and PASSWORDS).
 - Read access is restricted to Batch Job User Ids or STCs that execute the FTP jobs (could also be executed from as foreground job – need to restrict the program name maybe).
 - UPDATE access or higher is restricted to operations personnel that maintain the FTP job streams
 - AUDIT Controls for the datasets containing FTP login information are specified as SUCCESSES(UPDATES) FAILURES(UPDATES).
 - UACC (None) and NOWARNING are specified for the FTP login information data sets.
- d) Verify by doing the following:
 - 1. From the Administrator main menu, select 3.3 (Dataset Profile Reports) and press <ENTER>.
 - 2. Tab down to “Data Set” row, type LV next to the dataset profile for the FTP control information dataset.
 - 3. Check that UACC = None and Warning = No on the dataset profile
 - 4. Review the Universal Access and Access List on the dataset profile General Information Screen..
 - 5. Repeat steps 2 – 4, directly above, for all datasets containing FTP login information.
 - 6. If
 - a). Read access is restricted to STCs and Batch job user ids that execute the FTP jobs and
 - b). UPDATE access or higher is restricted to operations personnel responsible for maintaining FTP remote system logon/user id information. and
 - c) AUDIT (SUCCESSES(UPDATES), FAILURES (UPDATES)) is specified and
 - d) UACC = None and Warning = No, then there is NO FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

7. If any of the points in 6. above are not true, then there is a finding

CCI: CCI-000202

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ISLG0010

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that Syslogd is started at Z/OS system initialization.

NOTE: Syslogd may be started from the shell, a cataloged procedure (STC), or the BPXBATCH program. Additionally, other mechanisms (e.g., CONTROL-O) may be used to automatically start the Syslog daemon. To thoroughly analyze this PDI you may need to view the OS SYSLOG using SDSF, find the last IPL, and look for the initialization of Syslogd.

- a) If the Syslog daemon Syslogd is started automatically during the initialization of the z/OS system, there is NO FINDING.
- b) If (a) is untrue, this is a FINDING.

CCI: CCI-000764

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ISLG0020

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that Syslogd runs under its own user account. Specifically, it does not share the account defined for the Z/OS UNIX kernel.

The systems programmer responsible for supporting ICS will ensure that Syslogd runs with a job/started task name such as SYSLOGD that uniquely identifies it.

- 1) If you start SYSLOGD from MVS then ensure the following:
 - a) The SYSLOG daemon userid is SYSLOGD.
 - b) The SYSLOGD userid is defined as a PROTECTED userid.
 - c) The SYSLOGD userid has the following z/OS OMVS attributes: UID(0) HOME('/') PROGRAM('/bin/sh')
 - d) A matching entry in the STARTED class exists mapping the SYSLOGD started proc to the SYSLOGD userid.

To do the above:

Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the SYSLOGD started task. Document the USERID.

Using Vanguard Administrator User Profile summery mask on USERID = syslogd userid. Use the LV command and review the USERID and ensure all items are in effect for the Syslog daemon:

- 2) If you start SYSLOGD from /etc/rc then ensure the following:
 - a) The _BPX_JOBNAME and the BPX_USERID environment variables are set to the value 'SYSLOGD'.

To do the above:

You will need to locate the /etc/rc file and locate the BPX_JOBNAME and BPX_USERID in it.

- c) If SYSLOGD is started from MVS then if 1a) to 1d) are true, there is NO FINDING.
- e) If SYSLOGD is started from within MVS and 1a) to 1d) are untrue, this is a FINDING.
- f) If SYSLOGD is started from within USS and 2a) is true, this is NOT a FINDING.
- g) If SYSLOGD is started from within USS and 2a) is untrue, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ISLG0030**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the permission bits and user audit bits for HFS objects that are part of the Syslog daemon component are configured according to the settings in the following table:

SYSLOG DAEMON HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION BITS	USERAUDIT BITS
/usr/sbin/syslogd	1740	fff
/etc/syslog.conf	0744	faf

[Output log file defined in the configuration file]	0744	fff
---	------	-----

- a) Using Vanguard Administrator UNIX file manager option 14 review the files listed in the table above.
- b) If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in this table, there is NO FINDING.

NOTES:

The /usr/sbin/syslogd object is a symbolic link to /usr/lpp/tcpip/sbin/syslogd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The /etc/syslog.conf file may not be the configuration file the daemon uses. It is necessary to check the script or JCL used to start the daemon to determine the actual configuration file.

For example, in /etc/rc:

```
_BPX_JOBNAME='SYSLOGD' /usr/sbin/syslogd -f /etc/syslog.conf
```

For example, in the SYSLOGD started task JCL:

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT  
// PARM='POSIX(ON) ALL31(ON)/ -f /etc/syslogd.conf'
```

```
//SYSLOGD EXEC PGM=SYSLOGD,REGION=30M,TIME=NOLIMIT  
// PARM='POSIX(ON) ALL31(ON) /-f /"SYS1.TCPPARMS(SYSLOG)'"
```

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

7 rwx(least restrictive)
6 rw
3 -wx
2 -w-
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
-no auditing

c) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0010**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the TCP/IP started task's JCL specifies the PROFILE and SYSTCPD DD statements for the PROFILE.TCPIP and TCPIP.DATA configuration files and TCP/IP started task's JCL includes the RESOLVER_CONFIG variable, set to the name of the file specified on the SYSTCPD DD statement.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. If TCPIP is inactive, review the procedure libraries defined to JES2 and locate the TCPIP JCL member.
- b) Use IBM's dslist utility and review the TCPIP JCL to ensure the following items are in effect for the TCPIP started task JCL:
 - 1. The PROFILE and SYSTCPD DD statements specify the TCP/IP Profile and Data configuration files respectively.
 - 2. The RESOLVER_CONFIG variable on the EXEC statement is set to the same file name specified on the SYSTCPD DD statement.
- c) If both of the above are true, there is NO FINDING.
- d) If either of the above is untrue, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0020**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the TCPIPJOBNAME, HOSTNAME, DOMAINORIGIN, DATASETPREFIX, and NSINTERADDR statements are coded in the TCPIP.DATA file.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP.DATA configuration file.
- b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Data configuration file:
 - 1. TCPIPJOBNAME
 - 2. HOSTNAME
 - 3. DOMAINORIGIN/DOMAIN - Specifies the default domain name used for DNS searches.
 - 4. DATASETPREFIX
- c) If both of the above are true, there is NO FINDING.
- d) If either of the above is untrue, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0025**

Default Severity: Category II

The IAO will ensure that if any NSINTERADDR statements are coded in the TCPIP.DATA file, they refer to hosts connected directly to networks within the physical premises of the host site and located in areas with physical access limited to authorized personnel.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Refer to the Data configuration file specified on the SYSTCPD DD statement in the TCPIP started task JCL.
- b) Use IBM's dslist utility and review the TCPIP configuration file. Ensure the following items are in effect for the NSINTERADDR statements specified in the TCP/IP Data configuration file:
 - 1. The NSINTERADDR statements refer to hosts connected directly to networks within the physical premises of the host site.
 - 2. The NSINTERADDR statements refer to hosts that are located in areas with physical access limited to authorized personnel.
- c) If both of the above are true, there is NO FINDING.
- d) If either of the above is untrue, this is a FINDING.

CCI: CCI-000366

CCI: CCI-000919

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0030**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the DELETE statement is not coded in PROFILE.TCPIP files for production systems.

The systems programmer responsible for supporting ICS will ensure that the SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.

The systems programmer responsible for supporting ICS will ensure that the SMFPARMS statement is not used.

The systems programmer responsible for supporting ICS will ensure that the TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP.DATA configuration file.
- b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

- 1. The SMFPARMS statement is not coded or commented out.
- 2. The DELETE statement is not coded or commented out for production systems.
- 3. The SMFCONFIG statement is coded with (at least) the FTPCLIENT and TN3270CLIENT operands.
- 4. The TCPCONFIG and UDPCONFIG statements are coded with (at least) the RESTRICTLOWPORTS operand.

NOTE: If the INCLUDE statement is coded, the data set specified will be checked for access authorization compliance in STIG ID ITCP0070.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- c) If all of the above are true, there is NO FINDING.
- d) If any of the above is untrue, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0040**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the permission bits and user audit bits for HFS objects that are part of the Base TCP/IP component are configured according to the settings in the following table:

DIRECTORY or FILE	PERMISSION BITS	USERAUDIT BITS
/etc/hosts	0744	faf
/etc/protocol	0744	faf
/etc/resolv.conf	0744	faf
/etc/services	0740	faf
/usr/lpp/tcpip/sbin	0755	faf
/usr/lpp/tcpip/bin	0755	faf

- a) Using Vanguard Administrator UNIX File Manager option 14. Review all files located in the table above.
- b) If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in this table, there is NO FINDING.

NOTE: Some of the files listed above are not used in every configuration.
Absence of a file will not be considered a FINDING.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx(least restrictive)
6 rw
3 -wx
2 -w
5 r-x
4 r-
1 --x
0 --- (most restrictive)

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
-no auditing

c) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0050**

Default Severity: Category III

The IAO will ensure that the SERVAUTH resource class is mapped to the STIG required resource type SER.

The IAO will ensure that the generic resource EZA, EZB and IST. are defined to the SERVAUTH resource class and no access is specified.

The IAO will ensure that only authenticated users are permitted access to the network (NETACCESS), port (PORTACCESS), stack (STACKACCESS), CSSMTP, and FTP resources in the SERVAUTH class.

The IAO will ensure that the default access to EZA, EZB and IST-prefixed resources in the SERVAUTH class is no access.

NOTE: This FINDING only pertains to domains running Z/OS Version 2 Release 10 or above, including all releases of z/OS. If the domain being reviewed is not running at the required OS release, this FINDING will be marked NOT APPLICABLE.

- a) Using Vanguard Administrator General Resource Profile report option 3;4.
Mask on class = SERVAUTH
- b) Ensure the following items are in effect for Server Access Authorization resources:
 - 1. The following resources are defined to the SERVAUTH resource class with a UACC(NONE):
 - EZA.**
 - EZA.FTP.**
 - EZA.NETACCESS.**
 - EZA.PORTACCESS.**
 - EZA.STACKACCESS.**
 - EZB.**
 - EZB.FTP.**
 - EZB.NETACCESS.**
 - EZB.PORTACCESS.**
 - EZB.STACKACCESS.**If CSSmtp is on the system, the following resource must be defined for use by the CSSMTP started task and authenticated users for email services:
 - EZB.CSSMTP.sysname.writename.JESnode
 - IST.**
 - IST.FTP.**
 - IST.NETACCESS.**

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

IST.PORTACCESS.**
IST.STACKACCESS.**

2. No access is granted to EZA.**, EZB.**, AND IST.** (EZA.**, EZB.** and IST.** must be defined).
If the product CSSMTP is on the system, no access is given to EZB.CSSMTP
3. Only authenticated users are permitted access to the network (NETACCESS), port (PORTACCESS), stack (STACKACCESS), and FTP resources in the SERVAUTH resource class and email services (EXB.CSSMTP.sysname.writername.JESnode).

If CSSMTP is on the system, authenticated user access is indicated by ID(*) access of READ in the access list (this should not be true for EZA.**, EZB.** and IST.which cannot have any entries in the access list).
4. Ensure that the profile WARNING flag is OFF.
 - c) If all items in (b) are true, there is NO FINDING.
 - d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0060**

Default Severity: Category II

The IAO will ensure that the user account used for the TCP/IP address space is defined with the following characteristics:

- Named TCPIP or, in the case of multiple instances, prefixed with TCPIP
- Privilege to run as a started task
- z/OS UNIX attributes: UID(0), home directory '/', shell program /bin/sh

The IAO will ensure that the user account used for the EZAZSSI started task is defined with the following characteristics:

- Named EZAZSSI
- Privilege to run as a started task

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Record the USERID's associated with all the started tasks
- b) Ensure the following items are in effect for the userid(s) assigned to the TCP/IP address space(s):
 - 1. Named TCPIP or, in the case of multiple instances, prefixed with TCPIP
 - 2. Defined as a PROTECTED userid
 - 3. Z/OS UNIX attributes: UID(0), HOME directory '/', shell program /bin/sh
 - 4. A matching entry in the STARTED resource class exists enabling the use of the standard userid(s) and appropriate group
- c) Ensure the following items are in effect for the userid assigned to the EZAZSSI started task:
 - 1. Named EZAZSSI
 - 2. Defined as a PROTECTED userid
 - 3. A matching entry in the STARTED resource class exists enabling the use of the standard userid and appropriate group.
- d) If all of the items in (b) and (c) are true, there is NO FINDING.
- e) If any item in (b) or (c) is untrue, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCP0070**

Default Severity: Category II

The IAO will ensure that update, create, and scratch access to product data sets are restricted to systems programming personnel.

The IAO will ensure that update, create, and scratch access to the data set(s) containing the TCPIP.DATA and PROFILE.TCPIP configuration files are restricted to systems programming personnel and are logged.

The IAO will ensure that update, create, and scratch access to the data set(s) containing the configuration files shared by TCP/IP applications are restricted to systems programming personnel.

The IAO will ensure that write and allocate access to the data set(s) specified in the INCLUDE statements are restricted to systems programming personnel and are logged.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate and document the configuration file identified by the PROFILE DD statement. Locate and document the Data File identified by the SYSTCPD DD statement.

NOTE: Record the covering dataset profile for use in later steps.

- b) Ensure the following controls are in effect for the Base TCP/IP component:
 - a) Using Vanguard Administrator On-line Access and Authorization option 4. Supply the datasets documented above and ensure UPDATE and ALTER access to product data sets is restricted to systems programming personnel (i.e., SMP/E distribution data sets with the prefix SYS1.TCPIP.AEZA and target data sets with the prefix SYS1.TCPIP.SEZA).
 - b) Using Vanguard Administrator On-line Access and Authorization option 4. Supply the dataset names documented above. Review the access and ensure UPDATE and ALTER access to the data set(s) containing the Data and Profile configuration file is restricted to systems programming personnel.

NOTE: If any INCLUDE statements are specified in the Profile configuration file, the named MVS data sets have the same access authorization requirements.

- c) Using Vanguard Administrator Audit Flags Report option 3;3;2. Supply the datasets documented above. All UPDATE and ALTER access to the data set(s) containing the Data and Profile configuration files is logged.

NOTE: If any INCLUDE statements are specified in the Profile configuration file,

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

the named MVS data sets have the same logging requirements.

- d) Using Vanguard Administrator On-line Access and Authorization option
4. Supply the dataset name for the configuration file documented above.
Review the access and ensure UPDATE and ALTER access to the data
set(s) containing the configuration files shared by TCP/IP applications is
restricted to systems programming personnel.
- c) If all of the items in (b) are true, there is NO FINDING.
- d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITCPR052**

Default Severity: Category II

a) Using Vanguard Administrator select Security Server Commands

b) select Option 5 SETROPTS

c) Type an E in CDT classes and hit enter

CDT Classes:..... _ (E to edit data) *data is present*

d) Scroll down to SERVAUTH and check its status

if there are TCP/IP resources defined and the SERVAUTH resource class is active, there is NO FINDING.

If there are TCP/IP resources defined and the SERVAUTH resource class is not active, this is a FINDING.

CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITNT0010**

Default Severity: Category II

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.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP or TN3270 started task. Locate the configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the profile Data configuration file.
- b) Ensure the following items are in effect for the configuration statements specified in the Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

TELNETGLOBAL Block (only one defined)

1. The KEYRING statement, if used, is only coded within the TELNETGLOBALS statement block.
2. The KEYRING statement, if used, specifies the SAF parameter.

TELNETPARMS Block (one defined for each port the server is listening to, typically ports 23 and 992)

1. The TELNETPARMS INACTIVE statement is coded within each TELNETPARMS statement block and specifies a value between 1 and 900.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

NOTE: Effective in z/OS release 1.2, the INACTIVE statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

1. The TELNETPARMS TKOSPECLURECON statement is not coded or commented out.

BEGINVTAM Block (one or more defined)

2. The BEGINVTAM RESTRICTAPPL statement is not be coded or commented out.

c) If all of the above are true, there is NO FINDING.

d) If any of the above is untrue, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITNT0020**

Default Severity: Category II

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 DEFAULTAPPL 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 for systems at Z/OS 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.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP Data configuration file.
- b) Ensure the following items are in effect for the configuration statements specified in the TCP/IP Profile configuration file:

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

1. Within each BEGINVTAM statement block, one BEGINVTAM USSTCP statement is coded that specifies only the table name operand. No client identifier, such as host name or IP address, is specified so the statement applies to all connections not otherwise controlled.
2. The USS table specified on each “back stop” USSTCP statement mentioned in Item (1) above is coded to allow access only to session manager applications and NC-PASS applications. This check requires Manual Review.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

3. Within each BEGINVTAM statement block, additional BEGINVTAM USSTCP statements that specify a USS table that allows access to other applications may be coded only if the statements include a client identifier operand that references only secure terminals.
4. Any BEGINVTAM DEFAULTAPPL 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. This check requires Manual Review. IBM Communications Server Data Analysis
5. 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. This check requires Manual Review.

NOTE: The BEGINVTAM LINEMODEAPPL requirements will not be reviewed at this time. Further testing must be performed to determine how the CL/Supersession and NC-PASS applications work with line mode.

- c) If all of the above are true, there is NO FINDING.
- d) If any of the above is untrue, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITNT0030**

Default Severity: Category II

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.

- a) Display the active started tasks executing on the domain using SDSF, or equivalent JES display product, and locate the TCPIP started task. Locate the TCPIP configuration file identified by the PROFILE DD statement. From the ISPF Primary Option Menu use option 3.4 and review the TCPIP Date configuration file.
- b) Ensure that all USS tables referenced in BEGINVTAM USSTCP statements include MSG10 text that specifies a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

are private and confidential. See User Agreement for details.

c) If all the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITNT0050**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that a TELNETPARMS ENCRYPTION statement is coded for each statement block that defines a SECUREPORT and if the TELNETGLOBALS block includes an ENCRYPTION statement it has the correct cipher specifications.

The systems programmer responsible for supporting ICS will ensure that to prevent the use of null or 40-bit encryption, each TELNETPARMS ENCRYPTION statement or TELNETGLOBALS 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.

- a) Use SDSF or equivalent to locate the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL or the TN3270 started task JCL if configure separately in z/OS 1.8 and above.

NOTE: If the INCLUDE statement is coded in the TCP/IP profile configuration file, the data set specified on this statement must be checked for the following items as well.

- b) From the ISPF Primary Option Menu use option 3.4 and review the profile configuration file and ensure the following items are in effect for the configuration statements specified in the profile configuration file:
 - 1. Within each TELNETPARMS block that specifies a SECUREPORT statement, an ENCRYPTION statement is also coded.
 - 2. To prevent the use of non FIPS 140-2 encryption, each TELNETPARMS ENCRYPTION statement will specify any or all of the following operands:
 - a. SSL_3DES_SHA
 - b. SSL_AES_256_SHA
 - c. SSL_AES_128_SHA
 - 3. Within the TELNETGLOBALS block verify that if an ENCRYPTION statement is included it specifies any or all of the following cipher specifications to prevent the use of non FIPS 140-2 encryption:
 - a. SSL_3DES_SHA
 - b. SSL_AES_256_SHA
 - c. SSL_AES_128_SHA

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

c) If (B)1., (B)2., (B)3., above are true, there is NO FINDING.

d) If any of the above is untrue, this is a FINDING

CCI: CCI-000068

CCI: CCI-002450

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ITNT0060**

Default Severity: Category II

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.

- a) Using SDSF or equivalent, locate the Profile configuration file specified on the PROFILE DD statement in the TCPIP started task JCL or the TN3270 started task if configured separately in z/OS 1.8 and above.
- b) Using IBM's utility Dslist or equivalent locate the Profile configuration file and browse to review the file.

NOTE: If the INCLUDE statement is coded in the TCP/IP Profile configuration file, the data set specified on this statement must be checked for the following items as well.

- c) Ensure the following item is in effect for the configuration statements specified in the Profile configuration file:

-The TELNETPARMS SMFINIT and SMFTERM statements are coded with the TYPE119 operand within each TELNETPARMS statement block.

NOTE: Effective in z/OS release 1.2, the SMFINIT and SMFTERM statement can appear in both TELNETGLOBAL and TELNETPARM statement blocks.

- d) If the above is true, there is NO FINDING.
- e) If the above is untrue, this is a FINDING

CCI: CCI-000130

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IUTN0010**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the startup user account for otelnetd is the account defined for the Z/OS UNIX kernel.

- a) Using Vanguard Administrator UNIX File Manger option 14 use the CD command to change to the /etc directory and the browse command to review /etc/inetd.conf file.

```
#=====
# service | sock | prot | wait/ | user          | server          | server program
# name    | type |      | nowait|          | program         | arguments
#=====
otelnet   stream tcp   nowait OMVSKERN /usr/sbin/otelnetd otelnetd -m
```

- b) If the otelnetd command specifies OMVS or OMVSKERN as the user, there is NO FINDING. See example above
- c) If the otelnetd command specifies any user other than OMVS or OMVSKERN, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: IUTN0020

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the otelnetd startup command includes the options -D login and -c 900, where:

- D login indicates that messages should be written to the syslogd facility for login and logout activity
- c 900 indicates that the Telnet session should be terminated after 15 minutes of inactivity.

The systems programmer responsible for supporting ICS will ensure that the otelnetd startup command does not include the option -h, where:

- h indicates that the logon banner should not be displayed.

- a) Using Vanguard Administrator UNIX File Manager option 14. User the CD command to change to the etc directory and the browse the file /etc/inetd.conf
- b) Ensure the following items are in effect for the otelnetd startup command:
 - 1. Option -D login is included on the otelnetd command.
 - 2. Option -c 900 is included on the otelnetd command.

NOTE: 900 indicates a session timeout value of 15 minutes and is currently the maximum value allowed.

- 3. Option -h is not included on the otelnetd command.
- c) If all of the items in (b) are true, there is NO FINDING.
- d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-001133

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IUTN0030**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the /etc/banner file contains the warning logon.

- a) Using Vanguard Administrator UNIX file manager option 14 open use the CD command to change to the /etc directory and the browse command to review the /etc/banner file.
- b) Ensure the /etc/banner file contains a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. The thrust of this new policy is to make it clear that there is no expectation of privacy when using DoD information systems and all use of DoD information systems is subject to searching, auditing, inspecting, seizing, and monitoring, even if some personal use of a system is permitted:

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

c) If all the items in (b) above are true, there is NO FINDING.

d) If any item in (b) above is untrue, this is a FINDING.

CCI: CCI-000048

CCI: CCI-001384

CCI: CCI-001385

CCI: CCI-001386

CCI: CCI-001387

CCI: CCI-001388

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: IUTN0040**

Default Severity: Category II

The systems programmer responsible for supporting ICS will ensure that the permission bits and user audit bits for HFS objects that are part of the Z/OS UNIX Telnet Server component is configured according to the settings in the following table:

z/OS UNIX TELNET SERVER HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE PERMISSION BITS USER AUDIT BITS

/usr/sbin/otelnstd 1740 fff

/etc/banner 0744 faf

- a) Using Vanguard Administrator UNIX file manager option 14 open files browse files above and review Permission bits and USER Audit bits.
- b) If the HFS permission bits and user audit bits for each directory and file match or are more restrictive than the specified settings listed in the table above, there is NO FINDING.

NOTE: The /usr/sbin/otelnstd object is a symbolic link to /usr/lpp/tcpip/sbin/otelnstd. The permission and user audit bits on the target of the symbolic link must have the required settings.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7 rwx(least restrictive)
6 rw-
3 -wx
2 -w
5 r-x
4 r--
1 --x
0 --- (most restrictive)

The possible audit bits settings are as follows:

f log for failed access attempts
a log for failed and successful access
-no auditing

- c) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-000225

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

JES2 Data Analysis

___**STIG ID: ZJES0011**

Default Severity: Category II

Note that this guidance addresses RJE Workstations that are "Dedicated". If an RJE workstation is dedicated, the assumption is that the RJE to host connection is hard-wired between the RJE and host. In this case the RMT definition statement will contain the keyword **LINE=** which specifies that this RJE is only connected via that one **LINE** statement.

- a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.
- b) Review the workstation definitions by searching for **RMT**(in the member).
- c) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- d) Select option 1 User Profile. Change the * next to User ID to RMT* and press <ENTER>
- e) Print the screen(s) for use in check #1.
- f) Perform the following for each RJE workstation found:
- g) Enter "LR" command next to each userid on your list. Press <ENTER>
- h) Save the name of the dataset being browsed. Split screen, select option 1, and view the dataset from step h. Save it to your documentation library PDS. Note the PDS name and member name for use in check #2. Close the view session.
- i) Press <PF3> to get to the next userid and repeat the process from step h. When all userids have been processed, you will be returned to the userid list. Press <PF3> once more to return to Security Server Reports.
- j) Select option 17 ID in Access List. Press <ENTER>
- k) Select option 1 ID in Access List. Enter U next to ID Type, enter RMT* for ID Name, and enter B for Batch/Online. Press <ENTER> twice
- l) On the JCL Submit Processing panel, enter E on the command line.
- m) Change the REGION parameter on the execute card to 0M. Press <PF3>

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- n) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- o) Save the output
- p) For each RJE workstation definition found by searching for **RMT**(in step b perform the following:
 - 1. A userid of **RMTnnnn** is defined to RACF for *each* RJE workstation, where **nnnn** is the number on the **RMT** statement (review output from step e)
 - 2. No userid segments (e.g., TSO, CICS, etc.) are defined (review output from step h)
 - 3. Restricted from accessing all data sets and resources (review output from step o).
 - 4. NOTE: If no RJE workstations are defined to JES2, this is NOT APPLICABLE.
- q) If all of (p) is true, there is NO FINDING.
- r) If any of (p) is untrue, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0014**

Default Severity: Category II

- a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.
- b) Review the NJE definitions by searching for **NODE**(in the member. Note the NAME= parameter for each occurrence.
- c) Review the workstation definitions by searching for **RMT**(in the member).
- d) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- e) Choose Option 4 General Resource Profile Press <ENTER>
- f) Choose Option 1 General Resource Profile Summary AND put FACILITY next to class under Standard Masking Fields. Press <ENTER>
- g) Review the following resource definitions in the FACILITY resource class:

NJE.*
RJE.*
NJE.nodename
RJE.workstation

NOTE 1: Nodename is the NAME parameter value specified on the NODE statement. Review the JES2 parameters for NJE node definitions

NOTE 2: Workstation is RMTnnnn, where nnnn is the number on the RMT statement. Review the JES2 parameters for RJE workstation definitions

- h) If all JES2 defined NJE nodes and RJE workstations have a profile defined in the FACILITY resource class, there is NO FINDING
- i) If any JES2 defined NJE node or RJE workstation does not have a profile defined in the FACILITY resource class, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0021**

Default Severity: Category II

- a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.
- b) Review the spool offload receiver definitions by searching for **OFF**(in the member.
- c) Review the local card reader definitions by searching for **RDR**(in the member.
- d) Use the list of RJE workstations from ZJES0011 and the list of NJE nodes from ZJES012.
- e) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- f) Select option 4 General Resource Profile
- g) On the General Resources Reports panel, enter INTRDR in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>
- h) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- i) Save the output for use in the INTRDR (internal reader for batch jobs) check.
- j) Using the node list mentioned in step d, on the General Resources Reports panel, enter *nodename* in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>
- k) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- l) Save the output for use in the nodename (NJE node) check.
- m) Repeat step j through l for each nodename in the list
- n) On the General Resources Reports panel, enter OFF* in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- o) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- p) Save the output for use in the OFFn.* (spool offload receiver) check.
- q) On the General Resources Reports panel, enter R% % % %.* in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>
- r) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- s) Save the output for use in the Rnnnn (RJE workstation) check.
- t) On the General Resources Reports panel, enter RDR.* in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>
- u) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- v) Save the output for use in the RDRnn (local card reader) check.
- w) On the General Resources Reports panel, enter STCINRDR in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>
- x) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- y) Save the output for use in the STCINRDR (internal reader for started tasks jobs) check.
- z) On the General Resources Reports panel, enter TSUINRDR in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>
- aa) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- bb) Save the output for use in the TSUINRDR (internal reader for TSO logons) check.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

cc) From Administrator main Menu, select option 2 Security Server Commands.
Press <ENTER>

dd) From the VRC main menu, select option 5 SETROPTS. Press <ENTER>

ee) Under Class Options, enter E after CDT Classes. Press <ENTER>

ff) Enter *L JESINPUT* on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen and save it for the class active check.

gg) Review the following resources in the **JESINPUT** resource class:

- **INTRDR** (internal reader for batch jobs) – review output from step i.
- **nodename** (NJE node) – review output from step l.
- **OFFn.*** (spool offload receiver) – review output from step p.
- **Rnnnn** (RJE workstation) – review output from step s.
- **RDRnn** (local card reader) – review output from step v.
- **STCINRDR** (internal reader for started tasks) – review output from step y.
- **TSUINRDR** (internal reader for TSO logons) – review output from step bb.

NOTE: If any of these are not found, that resource in the **JESINPUT** resource class does not have to be defined.

hh) Ensure the following items are in effect:

1. The **JESINPUT** resource class is active (obtained in step ff).
2. The resources mentioned in step gg are protected by generic and/or fully qualified profiles defined to the **JESINPUT** resource class.
3. **UACC(NONE)** is specified for all resources.
4. **NOTE: UACC(READ)** is allowed for input sources that are permitted to submit jobs for *all* users. Currently, the *Z/OS STIG* provides no guidance on which input sources are appropriate for **UACC(READ)**. However, common sense should prevail during the analysis. For example, **UACC(READ)** would typically be inappropriate for RJE, NJE, offload, and STC input sources.

ii) If all of the items mentioned in (hh) are true, there is NO FINDING.

jj) If any of the items mentioned in (hh) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001310

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0022**

Default Severity: Category II

- a) From Administrator main Menu, select option 3 Security Server Reports;
Press <ENTER>
- b) Select option 4 General Resource Profile
- c) On the General Resources Reports panel, enter JESINPUT in the Class field
and enter B for Batch/Online. Select option 4 Access Lists and press
<ENTER>
- d) On the Processing Options Panel, enter Y for “Explode RACF groups in
access list at end of report?” and “Explode Users/Groups in Surrogate ID
access list at end of report?” Press <ENTER>
- e) On the JCL Submit Processing panel, enter S on the command line to submit
the job. Press <ENTER>
- f) Review the output to determine access authorization for resources defined to
the **JESINPUT** resource class.
- g) If access authorization for resources defined to the **JESINPUT** resource
class is restricted to the appropriate personnel, there is NO FINDING.
- h) **NOTE:** *Use common sense during the analysis. For example, access to
the offload input sources should be limited to systems personnel (e.g.,
operations staff).* If access authorization for any resource defined to the
JESINPUT resource class is inappropriate, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0031**

Default Severity:

- a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.
- b) Review the local printer definitions by searching for **PRT**(or **PRINTER** in the member.
- c) Review the local card definitions by searching for **PUN**(or **PUNCH** in the member.
- d) Review the remote workstation printer definitions by searching for **.PR** in the member.
- e) Review the remote workstation punch definitions by searching for **.PU** in the member.
- f) Use the list of NJE nodes from ZJES012 and the list of offload receivers from ZJES0021.
- g) From Administrator main Menu, select option 9 Analyzer. Press <ENTER>
- h) From Analyzer main menu, select 4 Batch Reports. Press <ENTER>
- i) From Batch Reports menu, select F Subsystem Name Table Analysis. Press <ENTER>
- j) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press <ENTER>
- k) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press <ENTER>
- l) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- m) Review the output. Note that the first entry in the report is the JES2 subsystem name and is typically JES2. This will be used in step p.
- n) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- o) Select option 4 General Resource Profile

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- p) In all profile names, replace **JES2** with the JES2 subsystem name determined in step m.
- q) On the General Resources Reports panel, enter **JES2.**** in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>
- r) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- s) Save the output for use in the **JES2.**** (backstop profile) check.
- t) On the General Resources Reports panel, enter **JES2.LOCAL.OFF%.*** in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>
- u) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- v) Save the output for use in the **JES2.LOCAL.OFFn.***, **JES2.LOCAL.OFFn.ST**, and **JES2.LOCAL.OFFn.JT** (spool offload related) checks.
- w) On the General Resources Reports panel, enter **JES2.LOCAL.PRT%** in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>
- x) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- y) Save the output for use in the **JES2.LOCAL.PRTn** ((local printer)) checks.
- z) On the General Resources Reports panel, enter **JES2.LOCAL.PUN%** in the Profile field, enter WRITER in the Class field and enter B for Batch/Online. Press <ENTER>
- aa) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- bb) Save the output for use in the **JES2.LOCAL.PUNn** (local punch) check.
- cc) Using the node list mentioned in step f, on the General Resources Reports panel, enter *nodename* in the Profile field, enter JESINPUT in the Class field and enter B for Batch/Online. Press <ENTER>

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- dd) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- ee) Save the output for use in the nodename (NJE node) check.
- ff) Repeat step u through w for each nodename in the list
- gg) On the General Resources Reports panel, enter **JES2.RJE.R%%%.P*** in the Profile field, enter **WRITER** in the Class field and enter B for Batch/Online. Press <ENTER>
- hh) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- ii) Save the output for use in the **JES2.RJE.Rnnnn.PRm** and **JES2.RJE.Rnnnn.PUm** (remote printer and punch) checks.
- jj) From Administrator main Menu, select option 2 Security Server Commands. Press <ENTER>
- kk) From the VRC main menu, select option 5 SETROPTS. Press <ENTER>
- ll) Under Class Options, enter E after CDT Classes. Press <ENTER>
- mm) Enter *L WRITER* on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen and save it for the class active check.
- nn) Review the following resources in the **WRITER** resource class where **JES2** is the name of the JES2 subsystem:
- **JES2.**** (backstop profile) – review output from step s.
 - **JES2.LOCAL.OFFn.*** (spool offload transmitter) – review output from step v.
 - **JES2.LOCAL.OFFn.ST** (spool offload SYSOUT transmitter) – review output from step v.
 - **JES2.LOCAL.OFFn.JT** (spool offload job transmitter) – review output from step v.
 - **JES2.LOCAL.PRTn** (local printer) – review output from step q.
 - **JES2.LOCAL.PUNn** (local punch) – review output from step t.
 - **JES2.NJE.nodename** (NJE node) – review output from step ee.
 - **JES2.RJE.Rnnnn.PRm** (remote printer) – review output from step ii.
 - **JES2.RJE.Rnnnn.PUm** (remote punch) – review output from step ii.
- NOTE: If any of these are not found, that resource in the **WRITER** resource class does not have to be defined.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

oo) Ensure the following items are in effect:

5. The **WRITER** resource class is active (obtained in step mm).
6. The resources mentioned in step nn are protected by generic and/or fully qualified profiles defined to the **WRITER** resource class.
7. **UACC(NONE)** is specified for all resources.
8. **NOTE: UACC(READ)** *is allowed for input sources that are permitted to submit jobs for **all** users. Currently, the **Z/OS STIG** provides no guidance on which input sources are appropriate for **UACC(READ)**. However, common sense should prevail during the analysis. For example, **UACC(READ)** would typically be inappropriate for RJE, NJE, offload, and STC input sources.*

pp) If all of the items mentioned in (oo) are true, there is NO FINDING.

qq) If any of the items mentioned in (oo) is untrue, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0032**

Default Severity: Category II

- a) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- b) Select option 4 General Resource Profile
- c) On the General Resources Reports panel, enter WRITER in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>
- d) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- e) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- f) Review the output to determine access authorization for resources defined to the **WRITER** resource class. The RACF resources include:
 - JES2.LOCAL.devicename
 - JES2.LOCAL.OFFn.*
 - JES2.LOCAL.OFFn.JT
 - JES2.LOCAL.OFFn.ST
 - JES2.LOCAL.PRTn
 - JES2.LOCAL.PUNn
 - JES2.NJE.nodename
 - JES2.RJE.devicename
- g) Access authorization for resources defined to the **WRITER** resource class will be restricted to operators and system programming personnel.

NOTE: Common sense should prevail during the analysis. For example, access to the offload output destinations should be limited to only systems personnel (e.g., operations staff/system programmers) on a classified system.
- h) The RACF resources and/or generic equivalent are defined with a default access of NONE.
- i) The RACF resource access authorizations are defined with UACC(NONE) and NOWARNING.
- j) If the above items g - i are true, there is NO FINDING.
- k) If any of the items g - i are not true, this is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

If the classification of the system is unclassified, this is not applicable.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0041**

Default Severity: Category II

- a) From Administrator main Menu, select option 2 Security Server Commands. Press <ENTER>
- b) From the VRC main menu, select option 5 SETROPTS. Press <ENTER>
- c) Under Class Options, enter E after CDT Classes. Press <ENTER>
- d) Enter *L JESSPOOL* on the command line. Note if there is a Y under the column labeled ACT. If yes, this indicates the class is active. Print the screen and save it for the class active check.
- e) Ensure that the **JESSPOOL** resource class is active (obtained in step d).
- f) If all of the items mentioned in (e) are true, there is NO FINDING.
- g) If any of the items mentioned in (e) is untrue, this is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0042**

Default Severity: Category II

- a) Determine the JES2PARM member as specified in the HASPPARM DD of the PROCLIB member used to start JES2.
- b) From Administrator main Menu, select option 9 Analyzer. Press <ENTER>
- c) From Analyzer main menu, select 4 Batch Reports. Press <ENTER>
- d) From Batch Reports menu, select F Subsystem Name Table Analysis. Press <ENTER>
- e) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press <ENTER>
- f) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press <ENTER>
- g) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- h) Review the output. Note that the first entry in the report is the JES2 subsystem name and is typically JES2. This will be used in step k.
- i) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- j) Select option 4 General Resource Profile
- k) In all profile names, replace **JES2** with the JES2 subsystem name determined in step h.
- l) On the General Resources Reports panel, enter **JES2.UPDATE.JESNEWS** in the Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online. Enter 2 on the command line to select Audit Flags and press <ENTER>
- m) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- n) Save the output for use in the **JES2.UPDATE.JESNEWS** audit checks.
- o) On the General Resources Reports panel, enter JESINPUT in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- p) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- q) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- r) Save the output for use in the **JES2.UPDATE.JESNEWS** audit checks.
- s) On the General Resources Reports panel, enter **JES2.UPDATE.JESNEWS** in the Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online. Press <ENTER>
- t) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- u) Save the output for use in the **JES2.UPDATE.JESNEWS** UACC checks.
- v) Ensure the following items are in effect:
 - 1. The **JES2.UPDATE.JESNEWS** resource is defined to the **OPERCMD**S resource class with a default access of NONE and all access is logged.
 - 2. Access authorization to the **JES2.UPDATE.JESNEWS** resource in the **OPERCMD**S class restricts CONTROL access to the appropriate personnel (i.e., users responsible for maintaining the JES News data set) and all access is logged.
- w) If both of the items in (v) are true, there is NO FINDING.
- x) If either item in (v) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001762

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0044**

Default Severity: Category II

- a) Use the list of NJE nodes from ZJES012 to determine the **localnodeid** by searching for **OWNNODE** in the NJEDEF statement, and then searching for **NODE(nnnn)** (where nnnn is the value specified by **OWNNODE**). The NAME parameter value specified on this NODE statement is the **localnodeid**.
- b) From Administrator main Menu, select option 9 Analyzer. Press <ENTER>
- c) From Analyzer main menu, select 4 Batch Reports. Press <ENTER>
- d) From Batch Reports menu, select F Subsystem Name Table Analysis. Press <ENTER>
- e) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press <ENTER>
- f) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press <ENTER>
- g) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- h) Review the output. Note that the first entry in the report is the JES2 subsystem name and is typically JES2. This will be used in step k.
- i) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- j) Select option 4 General Resource Profile
- k) In all profile names, replace **localnodeid** with the NAME parameter from the node determined as OOWNNODE in step a and replace **JES2** with the JES2 subsystem name determined in step h.
- l) On the General Resources Reports panel, enter **localnodeid.JES2.*** in the Profile field, enter JESSPOOL in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>
- m) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- n) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- o) Save the output for use in the *localnodeid.JES2.\$TRCLOG.taskid.*.JESTRACE* check.
- p) On the General Resources Reports panel, enter *localnodeid.+MASTER+.** in the Profile field, enter JESSPOOL in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>
- q) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- r) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- s) Save the output for use in the *localnodeid.+MASTER+.SYSLOG.jobid.*.SYSLOG** checks.
- t) Ensure that access authorization for the following resources:

localnodeid.JES2.\$TRCLOG.taskid..JESTRACE*
localnodeid.+MASTER+.SYSLOG.jobid..SYSLOG* or
localnodeid.+BYPASS+.SYSLOG.jobid.-.SYSLOG

is restricted to the following:

- 1. Userid(s) associated with external writer(s)
Ensure that access authorization for the resources mentioned is restricted to the following:

- 1. Userid(s) associated with external writer(s)
NOTE: An external writer is an STC that removes data sets from the JES spool. In this case, it is responsible for archiving the **JESTRACE** and **SYSLOG** data sets. The STC default name is **XWTR** and the external writer program is called **IASXWR00**.
- 2. Systems personnel and security administrators responsible for diagnosing JES2 and z/OS problems.

- u) If item (t) is true, there is NO FINDING.
- v) If item (t) is untrue, this is a FINDING

CCI: CCI-000213

CCI: CCI-001762

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZJES0046**

Default Severity: Category II

- a) Use the list of NJE nodes from ZJES012 to determine the **localnodeid** by searching for **OWNNODE** in the NJEDEF statement, and then searching for **NODE(nnnn)** (where nnnn is the value specified by **OWNNODE**). The NAME parameter value specified on this NODE statement is the **localnodeid**.
- b) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- c) Select option 4 General Resource Profile
- d) In all profile names, replace **localnodeid** with the NAME parameter from the node determined as OWNNODE in step a.
- e) On the General Resources Reports panel, enter **localnodeid.*** in the Profile field, enter JESSPOOL in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>
- f) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- g) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- h) Save the output for use in the **localnodeid.userid.jobname.jobid.dsnumber.name** check #1.
- i) On the General Resources Reports panel, enter **localnodeid.*** in the Profile field, enter JESSPOOL in the Class field and enter B for Batch/Online. Select option 2 Audit Flags and press <ENTER>
- j) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- k) Save the output for use in the **localnodeid.userid.jobname.jobid.dsnumber.name** check #3.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- l) Review the output from steps h and k for resource profiles with the following naming convention. These profiles may be fully qualified as indicated below or generic:
- ***localnodeid.userid.jobname.jobid.dsnumber.name***
 - ***localnodeid*** The name of the node on which the SYSIN or SYSOUT data set currently resides.
 - ***userid*** The userid associated with the job. This is the userid RACF uses for validation purposes when the job runs.
 - ***jobname*** The name that appears in the name field of the JOB statement.
 - ***jobid*** The job number JES2 assigned to the job.
 - ***dsnumber*** The unique data set number JES2 assigned to the spool data set. A **D** is the first character of this qualifier.
 - ***name*** The name of the data set specified in the DSN= parameter of the DD statement. If the JCL did not specify DSN= on the DD statement that creates the spool data set, JES2 uses a question mark (?).
- m) If the resources described in (l) are not present, there is NO FINDING.
- n) If the resources described in (l) are present, ensure the following items are in effect:
1. All users shall have access to their own JESSPOOL resources. This resource access does not require logging.
 2. The resource localnodeid.** will be restricted to only system programmers, operators and automated operations personnel, with access of ALTER. All access will be logged. (localnodeid. resource includes all generic and/or masked permissions, example: localnodeid.**, localnodeid.*, etc)
 3. The JESSPOOL localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked, can be made available to users when approved by the IAO. Access will be identified at the minimum access for the user to accomplish the users function. UPDATE, CONTROL, and ALTER access will be logged. An example is team members within a team, providing the capability to view, help, and/or debug other team member jobs/processes.
 4. CSSMTP ill be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the IAO. All access will be logged.
 5. Spooling products users (CMA-Spool, CA View, etc.) will be restricted to localnodeid.userid.jobname.jobid.dsnumber.name, whether generic and/or masked when approved by the IAO. Logging of access is not required.
- o) If all of the above are true, there is NO FINDING.
- p) If any of the above is untrue, this is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0052**

Default Severity: Category II

For this check please refer to JES2 system commands defined in the table entitled *Controls on JES2 System Commands* found in the U_zOS_STIG_Addendum,

- a) From Administrator main Menu, select option 9 Analyzer. Press <ENTER>
- b) From Analyzer main menu, select 4 Batch Reports. Press <ENTER>
- c) From Batch Reports menu, select F Subsystem Name Table Analysis. Press <ENTER>
- d) On the Subsystem Name Table Analysis panel, set the value for SORT CRITERIA to YES and other values to NO. Press <ENTER>
- e) On the SORT SELECTIONS panel, enter 1 next to SEQ. Press <ENTER>
- f) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- g) Review the output. Note that the first entry in the report is the JES2 subsystem name and is typically JES2. This will be used in step j.
- h) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- i) Select option 4 General Resource Profile
- j) In all profile names, replace **JES2** with the JES2 subsystem name determined in step g.
- k) On the General Resources Reports panel, enter **JES2.*** in the Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>
- l) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- m) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- n) Save the output for use in the **JES2.*** access list check.
- o) On the General Resources Reports panel, enter **JES2.*** in the Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online. Enter 2

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- on the
command line to select Audit Flags and press <ENTER>
- p) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
 - q) Save the output for use in the **JES2.*** audit check.
 - r) On the General Resources Reports panel, enter **JES2.*** in the Profile field, enter OPERCMDS in the Class field and enter B for Batch/Online. Press <ENTER>
 - s) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
 - t) Save the output for use in the **JES2.*** UACC check.
 - u) If the **JES2.**** resource is defined to the **OPERCMDs** class with a default access of NONE and all access is logged, there is NO FINDING.
 - v) If access to JES2 system commands defined in the table entitled *Controls on JES2 System Commands* found in the U_zOS_STIG_Addendum, is restricted to the appropriate personnel (e.g., operations staff, systems programming personnel, general users), there is NO FINDING.

NOTE: Use the **Auth** category specified in the table below as a guideline to determine appropriate personnel access to system commands.

- w) If access to specific JES2 system commands is logged as indicated in the table entitled *Controls on JES2 System Commands* below as indicated in the **LOG** column, below, there is NO FINDING.

If either (b), (c), or (d) above is untrue for any JES2 system command resource, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZJES0060**

Default Severity: Category II

- a) From Administrator main Menu, select option 3 Security Server Reports; Press <ENTER>
- b) Select option 4 General Resource Profile
- c) On the General Resources Reports panel, enter *.SUBMIT in the Profile field, enter SURROGAT in the Class field and enter B for Batch/Online. Select option 4 Access Lists and press <ENTER>
- d) On the Processing Options Panel, enter Y for “Explode RACF groups in access list at end of report?” and “Explode Users/Groups in Surrogate ID access list at end of report?” Press <ENTER>
- e) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- f) Save the output for use in the *executionuserid*.SUBMIT access list check.
- g) On the General Resources Reports panel, enter *.SUBMIT in the Profile field, enter SURROGAT in the Class field and enter B for Batch/Online. Enter 2 on the command line to select Audit Flags and press <ENTER>
- h) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- i) Save the output for use in the *executionuserid*.SUBMIT audit check.
- j) On the General Resources Reports panel, enter *.SUBMIT in the Profile field, enter SURROGAT in the Class field and enter B for Batch/Online. Press <ENTER>
- k) On the JCL Submit Processing panel, enter S on the command line to submit the job. Press <ENTER>
- l) Save the output for use in the *executionuserid*.SUBMIT UACC check.
- m) If no *executionuserid*.SUBMIT resources are defined to the **SURROGAT** resource class, there is NO FINDING.
- n) If *executionuserid*.SUBMIT resources are defined to the **SURROGAT** resource class, ensure the following items are in effect regarding surrogate controls:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- o) All **executionuserid.SUBMIT** resources defined to the **SURROGAT** resource class specify a default access of NONE.
- p) All resource access is except for scheduling tasks.
- q) Access authorization is restricted to scheduling tools, started tasks or other applications required for running production jobs.
- r) Other users may have minimal access required for running production jobs with documentation properly approved and filed with the site security official (ISSM or equivalent).
- s) If all of the items in (n) are true, there is NO FINDING.
- t) If any item in (n) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002233

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

DFSMS Data Analysis

___**STIG ID: ZMSR008**

Default Severity: Category II

- a) Generate a batch report of ACTIVE RACF CLASSES using Analyzer.
Review the output.
 - 1. Option 4 Batch Reports, from the Analyzer main menu
 - 2. Option 1: Class Descriptor Table Analysis
 - 3. Submit the job.
- b) Verify the following are classes are **ACTIVE - MGMTCLAS, STORCLAS, PROGRAM, and FACILITY** resources classes.
- c) Verify the following classes are **RACLISTED - MGMTCLAS and STORCLAS** resource classes.
- d) If (b) and (c) are true, there is NO FINDING.
- e) If (b) or (c) is not true, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZSMS0010**

Default Severity: Category II

- a) Generate a report of FACILITY class profiles beginning with STGADMIN, using the Administrator QUICK GEN utility.
 1. Option 3 Security Server Reports from the Administrator main menu.
 2. Option 4 General Resource Profile.
 3. Under the standard masking fields
Profile: STGADMIN*
Class: FACILITY
 4. Enter command option 1
 5. At the resulting profile list enter command option QG
 6. On line 1 in the edit field enter the following:
rlist &CLASS (&PROFILE) all
 7. On the command line enter GEN
 8. Enter VRABATCH. This will submit a batch job. Review the report.
- b) Ensure that the following items are in effect:
 1. The **STGADMIN.**** profile in the **FACILITY** resource class has a default access of NONE and grants no access at this level.
 2. **STGADMIN.DPDSRN.olddsname** is restricted to System Programmers only.
 3. The **STGADMIN.IGD.ACTIVATE.CONFIGURATION** is restricted to System Programmers.
 4. The **STGADMIN.IGG.DEFDEL.UALIAS** is restricted to System Programmers and Centralized and Decentralized Security personnel.
 5. The **STGADMIN.IGG.CATALOG.SECURITY.CHANGE** is defined with access of NONE and all access logged.
Note: the resource STGADMIN.IGG.CATALOG.SECURITY.CHANGE can be defined with read access for migration purposes. If it is a detailed migration plan it must be documented and filed by the ISSM that determines a definite migration period. All access must be logged. At the completion of migration this resource must be configured with access = NONE.

NOTE: The following STGADMIN resource profiles may be allocated to the enduser resulting in NO FINDING:

STGADMIN.ADR.COPY.CNCURRNT
STGADMIN.ADR.COPY.FLASHCPY
STGADMIN.ADR.COPY.TOLERATE.ENQF
STGADMIN.ADR.DUMP.CNCURRNT
STGADMIN.ADR.DUMP.TOLERATE.ENQF
STGADMIN.ADR.RESTORE.TOLERATE.ENQF

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

STGADMIN.ARC.ENDUSER
STGADMIN.IGG.ALTER.SMS

6. The STGADMIN resource profiles below are restricted to System programmers, DASD managers and Application Production Support Team members.
For STGADMIN.IDC.DCOLLECT, Automated Operations can have access also.

STGADMIN.ARC.CANCEL
STGADMIN.ARC.LIST
STGADMIN.ARC.QUERY
STGADMIN.ARC.REPORT
STGADMIN.DMO.CONFIG STGADMIN
STGADMIN.IDC.DCOLLECT
STGADMIN.IFG.READVTOC
STGADMIN.IGG.DELGDG.FORCE

7. STGADMIN resource profiles are controlled using the first **two** high-level resource name qualifiers (as below) at a minimum and restricted to System programmers and DASD managers.

STGADMIN.ADR
STGADMIN.ANT
STGADMIN.ARC
STGADMIN.DMO
STGADMIN.ICK
STGADMIN.IDC
STGADMIN.IFG
STGADMIN.IGG
STGADMIN.IGWSHCDS

8. The following Storage Administrator functions are controlled using the first **three** high-level resource name qualifiers at a minimum; restricted to System programmers and DASD managers and all access is logged.

STGADMIN.ADR.STGADMIN.BUILD SA
STGADMIN.ADR.STGADMIN.COMPRESS
STGADMIN.ADR.STGADMIN.COPY
STGADMIN.ADR.STGADMIN.COPY.DELETE
STGADMIN.ADR.STGADMIN.COPY.RENAME
STGADMIN.ADR.STGADMIN.DEFRAG
STGADMIN.ADR.STGADMIN.DUMP

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

STGADMIN.ADR.STGADMIN.DUMP.DELETE
STGADMIN.ADR.STGADMIN.PRINT
STGADMIN.ADR.STGADMIN.RELEASE
STGADMIN.ADR.STGADMIN.RESTORE
STGADMIN.ADR.STGADMIN.RESTORE.RENAME

9. All access to the following STGADMIN resources is logged:

STGADMIN.DPDSRN.olddsname
STGADMIN.IGG.DEFDEL.UALIAS
STGADMIN.IGD.ACTIVATE.CONFIGURATION

- c) If all items in (b) above are true, there is NO FINDING.
- d) If any item in (b) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZSMS0012**

Default Severity: Category II

- a) Generate a report using Administrator, of the PROGRAM resource class.
 1. Option 3 Security Server Reports, from the Administrator main menu
 2. Option 4 General Resource Profile
 3. Under the standard masking fields
Profile: DGT*
Class: PROGRAM
 4. Enter command option 1
 5. At the resulting profile list enter command option QG
 6. On line 1 in the edit field enter the following:
rlist &CLASS (&PROFILE) all
 7. On the command line enter GEN
 8. Enter VRABATCH. This will submit a batch job. Review the report.
- b) Review the **DGT*** profile in the **PROGRAM** resource class.
- c) If the **DGT*** profile has a default access of NONE and is restricted to appropriate personnel as defined in the table SMS Program Requirement found in the U_zOS_STIG_Addendum, there is NO FINDING.
- d) If the **DGT*** profiles restrict access to appropriate personnel as defined in the table SMS Program Requirement found in the U_zOS_STIG_Addendum, there is NO FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZSMS0020**

Default Severity: Category II

- a) Refer to the following item gathered from the Data Facility Storage Management Subsystem (DFSMS) Worksheet in the Preliminary Information Worksheets in Appendix B:

___ 1. Provide the following DFSMS data set names:

SCDS: _____

ACDS: _____

COMMDS: _____

ACS: _____

ACDS Backup: _____

COMMDS Backup: _____

- b) Generate a report for security verification using Analyzer.
1. Select option 4 Batch Reports from the Analyzer main menu
 2. Select option B Sensitive and Critical Data Sets Analysis
 3. Enter 'R' on line item "User defined list"
 4. Provide a dataset name or your choice which will include the names of the data sets gathered from step a) above.
Note: This may be a sequential data set or a PDS member
 5. Specify the options as listed here.

AC(1) module list ===> NO Duplicate Module Analysis ===> NO
RACF detail ===> YES Exceptions only ===> NO
RACF Group detail ===> YES
Search criteria ===> NO
Sort criteria ===> NO

6. Press enter to invoke the JCL Submit Processing
7. Enter 'S' to submit the batch report
8. Review the report for findings

Note: At the discretion of the ISSM, DASD administrators are allowed UPDATE access to the control datasets.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- c) Review the logical parmlib data sets, example:
SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names
for the following SMS data sets:

Source Control Data Set (SCDS)

Active Control Data Set (ACDS)

Communications Data Set (COMMDS)

Automatic Class Selection Routine Source Data Sets (ACS)

ACDS Backup

COMMDS Backup

- d) If the RACF data set rules for the **SCDS**, **ACDS**, **COMMDS**, and **ACS** data sets restrict UPDATE and ALTER access to only Z/OS systems programming personnel, there is NO FINDING.
- e) If the RACF data set rules for the **SCDS**, **ACDS**, **COMMDS**, and **ACS** data sets do not restrict UPDATE and ALTER access to only Z/OS systems programming personnel, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZSMS0022**

Default Severity: Category II

- a) Review the logical parmlib data sets, example:
SYS1.PARMLIB(IGDSMSxx), to identify the fully qualified file names
for the following SMS data sets:

Active Control Data Set (ACDS)
Communications Data Set (COMMDS)

Refer to the report produced in previous PDI(ZMSMR020) for the data set volume
serial number:

Refer to the following item gathered from the Data Facility Storage Management
Subsystem (DFSMS) Worksheet in the Preliminary Information Worksheets in
appendix B:

- ___ 1. Provide the following DFSMS data set names:

SCDS: _____

ACDS: _____

COMMDS: _____

ACS: _____

ACDS Backup: _____

COMMDS Backup: _____

- b) If the **COMMDS** and **ACDS** SMS data sets identified in (a) above reside on
different volumes, there is **NO FINDING**.
- c) If the **COMMDS** and **ACDS** SMS data sets identified in (a) above are
collocated on the same volume, this is a **FINDING**.

CCI: CCI-000549

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZSMS0030**

Default Severity: Category II

- a) Review the logical parmlib data sets, example:
SYS1.PARMLIB(IEFSSNxx), for one of the following SMS parameter settings:

1. Keyword syntax:

SUBSYS SUBNAME(SMS) INITRTN(IGDSSIIN)

2. Positional syntax:

SMS, IGDSSIIN

- b) If the required parameters are defined, there is NO FINDING.
- c) If the required parameters are not defined, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZSMS0032**

Default Severity: Category II

- a) Review the logical parmlib data sets, example:
SYS1.PARMLIB(IGDSMSxx), for the following SMS parameter settings:

Parameter Key

SMS

ACDS(*ACDS data set name*)

COMMDS(*COMMDS data set name*)

- b) If the required parameters are defined, there is NO FINDING.
- c) If the required parameters are not defined, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

TSO Data Analysis

___STIG ID: ZTSO0020

Default Severity: Category I

- a) From Analyzer main menu, go to 4;U.

Note: Analyzer 8.1 with PTF VS48081 is required for this option to be available.

- b) Set “Exceptions only” field to NO. Press <ENTER>.
- c) Submit the report.
- d) Review the generated report.
- e) If SYS1.UADS userids are limited and reserved for emergency purposes only, there is NO FINDING.
- f) If any SYS1.UADS userids are assigned for other than emergency purposes, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZTSO0030**

Default Severity: Category II

- a) From Administrator main menu, go to 3;4.
- b) In the Batch/On-line field key in B. In the Class field key in TSOAUTH. On the command line key in 4 (for the Access Lists report). Press <ENTER>. Accept the processing options by pressing <ENTER>. Submit the report.
- c) Review the GENERAL RESOURCE ACCESS LISTS report ensuring the following items are in effect:
 - 1. The ACCT authorization is restricted to security personnel.
 - 2. The CONSOLE authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.) and READ access may be given to all users if SDSF is installed (at the IAOs discretion).
 - 3. The MOUNT authorization is restricted to DASD batch users only.
 - 4. The OPER authorization is restricted to authorized systems personnel (e.g., systems programming personnel, operations staff, etc.).
 - 5. The PARMLIB authorization is restricted to only systems programming personnel and READ access may be given to audit users.
 - 6. The TESTAUTH authorization is restricted to only z/OS systems programming personnel.
- d) If all of the above are true, there is NO FINDING.
- e) If any of the above is untrue, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

UNIX System Services Data Analysis

___**STIG ID: ZSSH0010**

Default Severity: Category I

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) If SSH Daemon is not active, there is NOFINDING.
- d) Examine SSH daemon configuration file.
 - 1. If variable 'Protocol 2' is defined, there is NO FINDING.
 - 2. If variable 'Protocol' is defined in a leading comment or has a value other than 2, this is a FINDING.

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZSSH0020**

Default Severity: Category I

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) Examine SSH daemon configuration file **sshd_config**.
 - 1. If there are no Ciphers lines or the ciphers list contains any cipher not starting with “3des” or “aes”, this is a FINDING.
 - 2. If the Macs line is not configured to “hmac-shal” or greater, this is a FINDING.
- d) Examine the z/OS-specified sshd server system-wide configuration **zos_sshd_config**.
 - 1. If any of the following is untrue, this is a FINDING.
 - i. FTPSMODE YES
 - ii. CipherSource ICSF
 - iii. MACsSource ICSF

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZSSH0030**

Default Severity: Category II

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) If SSH Daemon is not active, there is NO FINDING.
- d) Examine SSH daemon configuration file.
 - 1. If Banner statement is missing or configured to none, this is a FINDING.
 - 2. Ensure that the contents of the file specified on the banner statement contain a logon banner. The below banner is mandatory and deviations are not permitted except as authorized in writing by the DoD Chief Information Officer. If there is any deviation, this is a FINDING.

STANDARD MANDATORY DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZSSH0040

Default Severity: Category II

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) If SSH Daemon is not active, there is NO FINDING.
- d) Examine SSH daemon configuration file.
 - 1. If Server SMF is not coded with ServerSMF TYPE119_U83, this is a FINDING.
 - 2. If Server SMF is commented out, this is a FINDING

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZSSH0050

Default Severity: Category II

- a) From Vanguard Administrator, choose Option 14; Vanguard Unix Manager, then Option 2; Unix File Manager.
- b) Locate the SSH daemon configuration file. This file may be found in the /etc/ssh/ directory.
- c) If SSH Daemon is not active, there is NO FINDING.
- d) Examine SSH daemon configuration file. Ensure the following are either not coded or commented out:


```
#HostKey for protocol version 1  
#HostKey /etc/ssh/ssh_host_key  
#HostKeys for protocol version 2  
#HostKey /etc/ssh/ssh_host_rsa_key  
#HostKey /etc/ssh/ssh_host_dsa_key
```
- e) Locate the z/OS-specific sshd server system wide configuration file zos_sshd_config. This file may be found in the /etc/ssh/ directory. Ensure that a HostKeyRingLabel line is coded and commented out.
- f) If either of the above is true, this is a FINDING.

CCI:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0011**

Default Severity: Category II

The Systems Programmer will ensure parmlib member IEASYSxx specifies parameter OMVS and does not specify OMVS=DEFAULT.

- a) Using Vanguard Analyzer online display select Parmlib Analysis option 3;L. When Parmlib options are displayed press enter to continue. When the Parmlib member list is presented locate the IEASYSxx member and browse this member.

NOTE: If the OMVS statement is not specified, OMVS=DEFAULT is used. This will result (as of Z/OS Release 2.8) in the Z/OS UNIX kernel starting in minimum configuration mode. In minimum mode there is no access to permanent file systems or to the shell, and IBM's Communication Server TCP/IP will not run.

- b) If the parameter is specified as OMVS=xx or OMVS=(xx,xx,...) in the IEASYSxx member, there is NO FINDING.
- c) If the parameter is not specified as OMVS=xx or OMVS=(xx,xx,...), this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0012**

Default Severity: Category II

The Systems Programmer will ensure parmlib member BPXPRMxx follows the specifications specified for the above control parameters SUPERUSER, STEPLIBLIST, USERIDALIASTABLE, STARTUP_PROC, and MOUNT.

- a) Use Vanguard Analyzer Parmlib Analysis option L. Browse all the BPXPRMxx members.
- b) Review the logical parmlib data sets, example:
SYS1.PARMLIB(BPXPRMxx), for the following UNIX Parameter Keywords and Values:

Parameter Keyword Value
SUPERUSER BPXROOT
TTYGROUP TTY
STEPLIBLIST (optional) /etc/steplib
If specified will use the above value.
USERIDALIASTABLE Will not be specified.
ROOT SETUID will be specified
MOUNT NOSETUID or (SETUID (for Vendor-provided files)) &
SECURITY (Specified regardless of Vendor-provided or not)
STARTUP_PROC OMVS

- c) If the required parameter keywords and values are defined, there is NO FINDING.
- d) If the required parameter keywords and values are not defined, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0013**

Default Severity: Category II

The Systems Programmer will ensure that if the /etc/auto.master HFS FILE is used that each /etc/mapname file listed specifies NOSETUID and SECURITY, unless a letter justifying a specific exception is filed with the IAO.

- a) Use Vanguard Analyzer option 3-Online Displays, Parmlib Analysis option L. Browse the BPXPRMxx members

- b) Review the logical parmli data sets, example:

SYS1.PARMLIB(BPXPRMxx), for the following FILESYSTYPE entry:

FILESYSTYPE TYPE(AUTOMNT) ENTRYPOINT(BPXTAMD)

If the above entry is not found or is commented out in the BPXPRMxx member(s), this is NOT APPLICABLE.

NOTE: The /etc/auto.master HFS file (and the use of Automount) is optional. If the file does not exist, this is NOT APPLICABLE.

NOTE: The setuid parameter and the security parameter have a significant security impact. For this reason these parameters must be explicitly specified and not allowed to default.

- c) If each MapName file specifies the “NOSETUID” and “SECURITY” statements for each automounted directory, there is NO FINDING.
- d) If there is a deviation from the required values and documentation for the deviation exists, there is NO FINDING.

NOTE: security No disables security checking for file access. Security No is only allowed on test and development domains. setuid Yes allows a user to run under a different UID/GID identity. Justification documentation is required to validate the use of setuid Yes.

- e) If (c), or (d) above is untrue, this is a FINDING.

CCI: CCI-001762

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0014**

Default Severity: Category II

The Systems Programmer or IAO will ensure that the restricted network services specified in the /etc/inetd.conf file listed in the table below are disabled, unless a letter justifying the use of the restricted network service is on file with the IAO.

RESTRICTED NETWORK SERVICES

Service	Port
Chargen	19
Daytime	13
Discard	9
Echo	7
Exec	512
finger	79
shell	514
time	37
login	513
smtp	25
timed	525
nameserver	42
systat	11
uucp	540
netstat	15
talk	517
qotd	17
tftp	69

- a) Using Vanguard Administrator UNIX file manager option 14. Use the CD command to change to /etc directory and browse the **inetd.conf** file.
- b) If all the services in the table above are not found in or are commented out of the /etc/inetd.conf file, there is NO FINDING.
- c) If any of the Restricted Network Services defined above is specified, this is a FINDING.

CCI: CCI-000382

CCI: CCI-001762

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0015**

Default Severity: Category II

The Systems Programmer will ensure that the umask command is executed with a value of 077 and the LOGNAME variable is marked read-only for the /etc/profile file, exceptions are documented with the IAO.

- a) Using Vanguard Administrator UNIX file manager option 14 open /etc directory and brows the **profile** file
- b) If the final or only instance of the umask command in /etc/profile is specified as “umask 077”, there is NO FINDING.
- c) If the LOGNAME variable is marked read-only (i.e., “readonly LOGNAME”) in /etc/profile, there is NO FINDING.
- d) If (b) or (c), above is untrue, this is a FINDING.

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0016**

Default Severity: Category II

The Systems Programmer will ensure that any chmod or chaudit command specified in the /etc/rc file does not result in less restrictive security than what is specified in table below. The Systems Programmer will ensure that the _BPX_JOBNAME variable is set to match the daemon's name (e.g., inetd, syslogd)

- a) Using Vanguard Administrator UNIX file manager option 14. Use the CD command to change to the /etc directory and browse the rc file.
- b) If all of the chmod commands in /etc/rc do not result in less restrictive access than what is specified in the table entitled System Directory Security Settings and the table entitled System File Security Settings in table below there is NO FINDING.

NOTE: The use of chmod commands in /etc/rc is required in most environments to comply with the required settings, especially for dynamic objects such as the /dev directory.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

- 7 rwx(least restrictive)
- 6 rw
- 3 -wx
- 2 -w-
- 5 r-x
- 4 r--
- 1 --x
- 0 --- (most restrictive)

- c) If all of the chaudit commands in /etc/rc do not result in less auditing than what is specified in the table entitled System Directory Security Settings and the table entitled System File Security Settings in Section 2.5.2.5, Z/OS UNIX HFS Directories and Files, found in the U_zOS_STIG_Addendum, there is NO FINDING.

NOTE: The use of chaudit commands in /etc/rc may not be necessary. If none are found, there is NO FINDING.

The possible audit bits settings are as follows:

- f log for failed access attempts
- a log for failed and successful access
- no auditing

- d) If the _BPX_JOBNAME variable is appropriately set (i.e., to match daemon name)

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

as each daemon (e.g., syslogd, inetd) is started in /etc/rc, there is NO FINDING.

NOTE: If _BPX_JOBNAME is not specified, the started address space will be named using an inherited value. This could result in reduced security in terms of operator command access.

e) If (b), (c), or (d) above is untrue, this is a FINDING.

CCI: CCI-000366

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0021**

Default Severity: Category II

The Systems Programmer and IAO will ensure that BPX. Resources are properly protected and access is restricted to appropriate system tasks or systems programming personnel, unless a letter justifying additional access is filed with the IAO. The Systems Programmer and IAO will ensure that BPX. DAEMON resources are properly protected and access is restricted to appropriate system tasks or systems programming personnel, unless a letter justifying additional access is filed with the IAO

- a) Use Vanguard Administrator General Resource Report option 3;4 to review the FACILITY Class. Use Class Facility and Profile BPX.*.** for the masking.
- b) Review the following items for the FACILITY resource class, TYPE(FAC):
 - 1. The RACF rules for the BPX.** resource specify a default access of NONE.
 - 2. There are no RACF user access to the BPX.** resource.
 - 3. There is no RACF rule for BPX.SAFFASTPATH defined.
 - 4. The RACF rules for each of the BPX resources listed in the table GENERAL FACILITY CLASS BPX RESOURCES found in the U_zOS_STIG_Addendum, specify a default access of NONE.
 - 5. The RACF rules for each of the BPX resources listed in the table GENERAL FACILITY CLASS BPX RESOURCES found in the U_zOS_STIG_Addendum, restrict access to appropriate system tasks or systems programming personnel .
- c) If any item in (b) is untrue, this is a FINDING.
- d) If all items in (b) are true, this is NOT A FINDING.

CCI: CCI-000213

CCI: CCI-001764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0022**

Default Severity: Category I

The Systems Programmer and IAO will ensure that BPX.SRV.userid resources are properly protected and access is restricted to appropriate system tasks or systems programming personnel, unless a letter justifying additional access is filed with the IAO.

- a) Using Vanguard Administrator General Resource Report option 3;4 to review the FACILITY Class. Use Class Facility and Profile BPX.SRV.** for the masking.
- b) If the RACF rules for all BPX.SRV.user SURROGAT resources specify a default access of NONE, there is NO FINDING.
- c) If the RACF rules for all BPX.SRV.user SURROGAT resources restrict access to system software processes (e.g., web servers) that act as servers under Z/OS UNIX, there is NO FINDING.
- d) If (b) or (c) above is untrue, this is a FINDING

CCI: CCI-000213

CCI: CCI-002233

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZUSS0023

Default Severity: Category I

The IAO will ensure that the CHOWN.UNRESTRICTED resource is not defined, unless a letter justifying access is filed with the IAO. The IAO will ensure that all SUPERUSER resources for the UNIXPRIV resource class are restricted to appropriate system tasks and/or system programming personnel, unless a letter justifying access is filed with the IAO. And the IAO will ensure that all SUPERUSER resources for the UNIXPRIV resource class have default access of none.

- a) Using Vanguard Administrator General Resource Report's option 3; 4 to review profiles listed below. Use Class masking UNIXPRIV and browse the profile listed below.
- b) Review the following items for the UNIXPRIV resource class:
 - 1. The RACF rules for the SUPERUSER resource specify a default access of NONE.
 - 2. There are no RACF rules that allow access to the SUPERUSER resource.
 - 3. There is no RACF rule for CHOWN.UNRESTRICTED defined.
 - 4. The RACF rules for each of the SUPERUSER resources listed in the table UNIXPRIV CLASS RESOURCES found in the U_zOS_STIG_Addendum, specify a default access of NONE.
 - 5. The RACF rules for each of the SUPERUSER resources listed in the table UNIXPRIV CLASS RESOURCES found in the U_zOS_STIG_Addendum,, restrict access to appropriate system tasks or systems programming personnel.
- c) If any item in (b) is untrue, this is a FINDING.
- d) If all items in (b) are true, this is NOT A FINDING.

CCI: CCI-000213

CCI: CCI-001764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZUSS0031

Default Severity: Category II

(ZUSS0031: CAT II) The Systems Programmer and IAO will ensure that data set rules for the data sets referenced in the ROOT and MOUNT statements in BPXPRMxx member in. PARMLIB are properly restricted and access is restricted to appropriate system tasks or systems programming personnel, unless a letter justifying additional access is filed with the IAO.

- a) Use Vanguard Analyzer UNIX System Services Filesystems option 3;N to review current UNIX System Mount points Use the R command to review the dataset rules for each profile listed below.
- b) If the RACF data set rules for the data sets referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update access to the Z/OS UNIX kernel (i.e., OMVS or OMVSKERN) there is NO FINDING.
- c) If the RACF data set rules for the data set referenced in the ROOT and the MOUNT statements in BPXPRMxx restrict update and/or allocate access to systems programming personnel there is NO FINDING.
- d) If (b) or (c) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZUSS0032

Default Severity: Category II

The Systems Programmer and IAO will ensure that data set rules for the data sets referenced in the table A-19 are properly restricted and UPDATE and/or ALLOCATE/ALTER access is restricted to systems programming personnel, unless a letter justifying additional access is filed with the IAO.

- a) Use Vanguard Administrator Data Set Reports option 3;3 to review dataset profiles listed in the table above.
- b) If the RACF data set rules for each of the data sets listed in Section 2.5.2.4.1 MVS Data Sets with Z/OS UNIX Components, Table A-19, in the U_zOS_STIG_Addendum restrict UPDATE and ALTER access to systems programming personnel, there is NO FINDING.
- c) If (b) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0033**

Default Severity: Category II

The IAO will ensure that update and allocate access to libraries residing in the /etc/steplib is limited to system programmers only, unless a letter justifying access is filed with the IAO, all update and allocate access is logged.

- a) Use Vanguard UNIX file manager option 14. Use the CD command to change to the /etc directory and use the browse command to review file located in /etc/steplib
- b) The RACF data set rules for libraries specified in the STEPLIBLIST file allow inappropriate (e.g., global READ) access.
- c) The RACF data set rules for libraries specified in the STEPLIBLIST file do not restrict UPDATE and/or ALTER access to only systems programming personnel.
- d) The RACF data set rules for libraries specified in the STEPLIBLIST file do not specify that all (i.e., failures and successes) UPDATE and/or ALTER access will be logged.
- e) If all of the above are untrue, there is NO FINDING.
- f) If any of the above is true, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZUSS0034

Default Severity: Category II

The Systems Programmer will ensure that the HFS permission bits for each directory match or are more restrictive than the specified settings listed in the table A-21 entitled System Directory Security Settings in Section 2.5.2.5.1.

Use Vanguard UNIX file manager option 14 and review the files listed in Section 2.5.2.5.1 Z/OS System HFS Directories Table A21 found in the in the U_zOS_STIG_Addendum

If the HFS permission bits for each directory match or are more restrictive than the specified settings listed in Section 2.5.2.5.1, Z/OS System HFS Directories, Table A21, of the Z/OS STIG, there is NO FINDING.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

- 7 rwx(least restrictive)
- 6 rw
- 3 -wx
- 2 -w-
- 5 r-x
- 4 r--
- 1 --x
- 0 --- (most restrictive)

- a) If the HFS user audit bits for each directory match or include the specified settings listed in Section 2.5.2.5.1, Z/OS System HFS Directories, Table A-21, of the Z/OS STIG, there is NO FINDING.

The possible audit bits settings are as follows:

- f log for failed access attempts
- a log for failed and successful access
- no auditing

- b) If (b) or (c) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0035**

Default Severity: Category II

The Systems Programmer will ensure that the HFS user audit bits for each file match settings listed in the table A-22 entitled System File Security Settings in Section 2.5.2.5.2. found in the U_zOS_STIG_Addendum

NOTE: Some of the files listed in the referenced Z/OS STIG table are not used in every domain. If the file does not exist, there is NO FINDING.

- a) If the HFS permission bits for each file match or are more restrictive than the specified settings listed in Section 2.5.2.5.2, Z/OS System HFS Files, Table A-22, in the Z/OS STIG, there is NO FINDING.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

- 7 rwx(least restrictive)
- 6 rw-
- 3 -wx
- 2 -w-
- 5 r-x
- 4 r--
- 1 --x
- 0 --- (most restrictive)

- b) If the HFS user audit bits for each file match or include the specified settings listed in Section 2.5.2.5.2, Z/OS System HFS Files, Table A-22, of the Z/OS STIG, there is NO FINDING.

The possible audit bits settings are as follows:

- f log for failed access attempts
- a log for failed and successful access
- no auditing

- c) If (b) or (c) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0036**

Default Severity: Category II

The Systems Programmer will ensure that the HFS directory(ies) with the "other" write permission bit set is (are) not properly defined.

- a) If there are no directories that have the other write permission bit set on without the sticky bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the sticky bit is indicated as a “t” or “T” in the execute portion of the other permissions. For example, a display of the permissions of a directory with the sticky bit on could be “drwxrwxrwt”.

- b) If all directories that have the other write permission bit set on do not contain any files with the setuid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setuid bit is indicated as an “s” or “S” in the execute portion of the owner permissions. For example, a display of the permissions of a file with the setuid bit on could be “-rwsrwxrwx”.

- c) If all directories that have the other write permission bit set on do not contain any files with the setgid bit set on, there is NO FINDING.

NOTE: In the symbolic permission bit display, the setgid bit is indicated as an “s” or “S” in the execute portion of the group permissions. For example, a display of the permissions of a file with the setgid bit on could be “-rwxrwsrwx”.

- d) If (a), (b), or (c) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0041**

Default Severity: Category II

The Systems Programmer will ensure that the OMVSGRP group and / or the STCOMVS group are each defined to the security database with a unique GID in the range of 1-99.a)

- a) Review Vanguard Administrator Group OMVS Segment report 3;5;22

NOTE: A site can choose to have both an OMVSGRP group and an STCOMVS group or combine the groups under one of these names.

- b) If the OMVSGRP group and / or the STCOMVS group are each defined with a unique GID in the range of 1-99, there is NO FINDING.
- c) If (b) above is untrue, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0042**

Default Severity: Category II

The IAO will ensure each group has a unique GID number.

- a) Review Vanguard Administrator Group OMVS Segment report option: 3;5;22 sort on GID

NOTE: This check only applies to groups that include users of Z/OS UNIX (i.e., that have an OMVS segment defined).

- b) If each group has a unique GID number, there is NO FINDING.
- c) If more than one group has the same GID number, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZUSS0043

Default Severity: Category II

The Systems Programmer and IAO will ensure that the user account for the Z/OS UNIX kernel (OMVS) is properly defined to the security database.

- a) Review Vanguard Administrator User OMVS Segment report option 3;5;9 Mask
USERID=OMVS
- b) If OMVS is defined as follows, there is NO FINDING:
 - 1. No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
 - 2. Default group specified as OMVSGRP or STCOMVS
 - 3. UID(0)
 - 4. HOME directory specified as “/”
 - 5. Shell program specified as “/bin/sh”
- c) If OMVS is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0044**

Default Severity: Category II

The user account for the z/OS UNIX SUPERUSER userid must be properly defined.

- a) Review Vanguard Administrator USER OMVS Segment Report 3;5;9 Mask on
USERID=BPXROOT
- b) Refer to system PARMLIB member BPXPRMxx (xx is determined by OMVS
entry in IEASYS00.)
- c) If BPXROOT is defined as follows, there is NO FINDING:
 - 1. No access to interactive on-line facilities (e.g., TSO, CICS, etc.)
 - 2. Default group specified as OMVSGRP or STCOMVS
 - 3. UID(0)
 - 4. HOME directory specified as "/"
 - 5. Shell program specified as "/bin/sh"
- d) If BPXROOT is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0045**

Default Severity: Category II

The Systems Programmer and IAO will ensure that the RMFGAT user account is properly defined in the security database.

RMFGAT is the userid for the Resource Measurement Facility (RMF) Monitor III Gatherer. If RMFGAT is not defined this is not applicable.

- a) Review Administrator User OMVS Segment Report 3;5;9 Mask on
USERID=RMFGAT
- b) Enter an “LV” next to the UserID to display the user information. The
default group will be located under GENERAL INFORMATION; the
remainder of the information will be located under OMVS SEGMENT.
- c) If RMFGAT is defined as follows, there is NO FINDING:
 - 1. Default group specified as OMVSGRP or STCOMVS
 - 2. A unique, non-zero UID
 - 3. HOME directory specified as “/”
 - 4. Shell program specified as “/bin/sh”
- d) If RMFGAT is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0046**

Default Severity: Category I

The Systems Programmer and IAO will ensure that UID(0) is assigned only to system tasks such as the Z/OS UNIX kernel (i.e., OMVS or OMVSKERN), Z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons; to security administrators who create or maintain user account definitions; and to systems programming accounts dedicated to maintenance (e.g., SMP/E) of HFS-based components.

- a) Review Vanguard Administrator User OMVS Segment Report option 3;5;9 Mask on UID =0
- b) If UID(0) is assigned only to system tasks such as the Z/OS UNIX kernel (i.e., OMVS), Z/OS UNIX daemons (e.g., inetd, syslogd, ftpd), and other system software daemons; there is NO FINDING.
- c) If UID(0) is assigned to security administrators who create or maintain user account definitions; and to systems programming accounts dedicated to maintenance (e.g., SMP/E) of HFS-based components, there is NO FINDING.

NOTE: The assignment of UID(0) confers full time superuser privileges. As discussed in the Z/OS STIG, this is not appropriate for personal user accounts. Access to the BPX.SUPERUSER resource is used to allow personal user accounts to gain short-term access to superuser privileges.

- d) If UID(0) is assigned to non-systems or non-maintenance accounts, this is a FINDING.

CCI: CCI-000764

CCI: CCI-002235

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0047**

Default Severity: Category II

The Systems Programmer and IAO will ensure that each user account is defined with a unique UID number (except for UID(0) users), a unique HOME directory (except for UID(0) and other system task accounts), and shell program specified as "/bin/sh", "/bin/tcsh", or "/bin/false."

- a) Review Vanguard Administrator USER OMVS SEGMENT report option 3;5;9. Sort by UID.
- b) If each user account is defined as follows, there is NO FINDING:
 - 1. A unique UID number (except for UID(0) users)
 - 2. A unique HOME directory (except for UID(0) and other system task accounts)
 - 3. Shell program specified as "/bin/sh", "/bin/tcsh", "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

- c) If any user account is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0048**

Default Severity: Category II

The Systems Programmer and IAO will ensure that the below bulleted options are enforced for FTP socket applications using shared OMVS segments.

- Application of the APAR PQ63326 to control FTP access to UNIX files is required.
- Collection of SMF type 80 records to track user access to OMVS default UID.
- Use of the OMVS default UID will not be allowed on any classified system.
- The definition of the OMVS default user will be restricted to a non-0 UID, a non-writable home directory, such as "\" root, and a non-executable, but existing, binary file, "/bin/false" or "/bin/echo."

NOTE: This check only applies to the OMVS default user. If the OMVS default user is not defined in the Application Data field in the BPX.DEFAULT.USER resource in the FACILITY report, this is **NOT APPLICABLE**.

- a) Using Vanguard Administrator General Resource Profile report, mask on Profile=BPX.DEFAULT.USER and Class=Facility. Use the LV command to review this profile. Document the Appl Data (i.e. USERID/GROUPID) for later use.
- b) Repeat step a), masking on Profile=BPX.UNIQUE.USER.
- c) Using Vanguard Administrator User Report, mask on USER id=USERID (the OMVS default user) documented above in step a). Use the VRC command to view the user profile. Find the OMVS Segment Information and review. If OMVS default user account is defined as follows, there is NO FINDING.
 1. unique UID number (except for UID(0) users)
 2. A non-writable HOME directory
 3. Shell program specified as "/bin/echo", or "/bin/false"
- d) Repeat step c), masking on USER id=USERID (the OMVS unique user) documented above in step b). If OMVS unique user account is defined as follows, there is NO FINDING.
 1. unique UID number (except for UID(0) users)
 2. A non-writable HOME directory
 3. Shell program specified as "/bin/echo", or "/bin/false"

NOTE: The shell program must have one of the specified values. The HOME directory must have a value (i.e., not be allowed to default).

- e) If the user account is not defined as specified in (b) above, this is a FINDING.

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSS0080**

Default Severity: Category II

z/OS Software owning Shared accounts” maybe created for the installation and upgrades on the z/OS Mainframe products that require the use of USS (UNIX System Services) as long as all IA requirements are met. “z/OS USS Software Owning Shared Accounts” shall be referenced within this VUL as the full name or abbreviated “Shared accounts” for all references within this VUL.

A. If you do not have any shared ids for Unix System Services, there is NO FINDING.

B. If you DO have shared IDs, You must ensure the following:

Rules and requirements for z/OS USS Software Owning Shared Accounts.

1) Shall include a statement from the responsible SA requesting the “shared account”, stating specific justification for the z/OS USS Software Owning shared account. Responsible SA shall be responsible for maintaining all documentation concerning account, usage, control, annual review, etc and shall provide upon request by IA staff or auditors as requested.

B.1: Does the organization have a statement from the responsible SA requesting the shared account? YES _____ NO _____

2) A separate “z/OS USS Software Owning shared account” userid will be created for each application and/or product that requires USS for separation of duties for product support. This “shared account” shall be used for the sole purpose of file/directory ownership based upon the UID assigned to the “shared account”.

B.2: Are the shared userids kept separate for each application and/or product and used for the sole purposes of file/directory ownership based on the UID assigned for the shared account? YES _____ NO _____

3) The “shared accounts” shall only be used within/for USS (UNIX System Services). The “shared account” userids shall have no special privileges, will not be granted access to interactive on-line facilities, batch facility, and will not be granted access to datasets and resources outside of the USS environment.

B.3.a: Are these shared userids only used within Unix System Services?

YES _____ NO _____

B.3.b: For each Shared userid validate that it has no special privileges, no interactive on-line facilities access, no batch facility access and no access to datasets or resources outside of the USS environment:

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

1. For each Shared Userid do the following:
2. From the Administrator Main Menu choose Option 3.1 and type Live on the command line and hit enter, and then place the userid on the User ID: field and press enter.
3. View the generated REBUILD commands for each of the Shared Userids and validate the following:
 1. The userid has not been granted the RACF OPERATIONS, SPECIAL or AUDITOR attribute or any GROUP SPECIAL, OPERATIONS or AUDITOR attributes.
 2. No access to interactive on-line facilities (e.g., TSO) other than OMVS.
 3. The userid is restricted from accessing all data sets and resources with the following exceptions:
 - a. Datasets necessary for USS operations.
 - b. Resources necessary for USS operations.
 - c. Ensure that group connect are also limited to the above.

B.3.c: Are all of the above true for Shared ID access:

YES _____ NO _____

4) The “shared account” userids shall adhere to the same complex password syntax rules and shall be assigned a non-expiring complex password or be set up as protected under RACF.

Using the Rebuild done in step 3 above, ensure that either the userids has NOPASSWORD specified or NOINTERVAL. If NOINTERVAL then the userid must also have a complex password in accordance with check : RACF0460

B.4: Was the shared account userid created with either NOPASSWORD or NOINTERVAL and with a complex password in accordance with check RACF0460:

YES _____ NO _____

5) Authorized user(s) shall only access “shared account” via the USS “SU” Command (switch user: su -s userid) and not utilize any password. When the ACP IAO creates the account with a complex password, such password shall not be written down or shared with others.

B.5: Are only authorized users accessing these shared accounts via the SU command and no passwords written down or shared with others?

YES _____ NO _____

6) The responsible documented z/OS system programmer shall be granted specific limited and temporary access based upon submitted security service requests

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

identifying project, duration required and justification for accessing “shared account” via the “su” command on a specific z/OS domain, example: initial software installation or upgrade of specific vendor software.

B.6: Is the z/OS system programmer only granted limited and temporary access based on a submitted security request that identifies the project, duration required and justification for access the shared account via the su command on a specific z/OS Domain?:

YES _____ NO _____

7) Responsible individual z/OS System programmer shall be granted temporary access to the specific BPX.SRV.userid (“userid” shall be the single “shared account” requested) in the surrogate user class with full logging of the permission to BPX.SRV.userid for the specific period of time required to perform functional requirements via the “su” command and appropriate usage of the “shared account”.

B.7: To validate this, From the Administrator Main Menu choose Option 3.4 and type Live on the command line, hit enter, and then place on the Profile field: BPX.SVR* and on the CLASS field: Surrogat field and press enter.

Ensure each that shared ID is represented in the list as a profile of BPX.SRV.sharedid and then next to the profile on the CMD line type VRC and ensure the following:

1. UACC is None.
2. Warning is N
3. Audit Successes is READ
4. Audit Failures is READ
5. On the Standard Access Permits and Conditional Access Permits where * data is present* place an E on that line and validate that Only z/OS Systems Programmers allowed temporary access are in the access list with access greater than NONE.

B.7. a: Are all of the above true for Shared ID access:

YES _____ NO _____

8) Standard procedure for all updates within USS Directories/files shall be performed based upon the direct authority granted to the z/OS system programmer individual userids. Shared accounts shall only be utilized for initial software installation or vendor software upgrades.

B.8: Are Shared Userids only used for initial software installation and/or vendor software upgrades?

YES _____ NO _____

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

C. If you answered YES to all questions and requirements above, there is NO FINDING.

D. If you answered NO to any of the questions and requirements above, there is a FINDING.

CCI: CCI-000213

CCI: CCI-000770

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZUSSR050

Default Severity: Category II

The IAO will ensure that the BPX.DEFAULT.USER for the FACILITY resource class is only used for FTP socket applications on non classified systems.

If the system is not classified this is not applicable.

- a) Review System Classification General Resource Profile BPX.DEFAULT.USER Using Vanguard Administrator General Resource Reports option 3;4 Mask on Profile=BPX.DEFAULT.USER and class=FACILITY.
 - b) If system is classified or does not use the FTP socket application the Default User and Default Group are not defined in the Application Data field in the BPX.DEFAULT.USER resource in the FACILITY report, there is NO FINDING.
 - c) If the system is a non classified system, running the FTP socket application, and has Default User and Default Group defined in the Application Data field in the BPX.DEFAULT.USER resource in the FACILITY report, there is NO FINDING.
 - d) If (b) and (c) above are untrue, this is a FINDING.
- CCI:** CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSSR060**

Default Severity: Category II

The IAO will ensure that the ACTIVE CLASSES list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes.

- a) Review Vanguard Analyzer RACF Class Descriptor Table Analysis option 3; 1
- b) Ensure the following CLASSES list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes are listed as STATUS is ACTIVE, there is NO FINDING.
- c) If (b) above is untrue, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZUSSR070**

Default Severity: Category II

The IAO will ensure that the SETR RACLIST CLASSES list includes entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes.

- a) Review Vanguard Analyzer RACF Class Descriptor Table Analysis option 3; 1
- b) If the CLASSES listed include entries for the FACILITY, SURROGAT, and UNIXPRIV resource classes are listed as RACLIST = YES there is NO FINDING.
- c) If (b) above is untrue, this is a FINDING

CCI: CCI-000366

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

VTAM Data Analysis

___ **STIG ID: ZVTM0011**

Default Severity: Category II

- a) Refer to the following items gathered from the VTAM Systems Programmer's Worksheet in the Preliminary Information Worksheets in Appendix B:

- ___ 1. Documentation regarding terminal naming standards.
 - ___ 2. Documentation of all procedures controlling terminal logons to the system.
 - ___ 3. A complete list of all **USS** commands used by terminal users to log on to the system.
 - ___ 4. A complete list of all terminals and/or terminal types controlled by **LOGAPPL** definitions only.
 - ___ 5. Members and data set names containing **USSTAB** and **LOGAPPL** definitions of all terminals that can log on to the system (e.g., **SYS1.VTAMLST**).
 - ___ 6. Members and data set names containing logon mode parameters.
- b) If **USSTAB** definitions are only used for secure terminals (e.g., terminals that are locally attached to the host or connected to the host via secure leased lines), there is **NO FINDING**.
- c) If **USSTAB** definitions are used for any unsecured terminals (e.g., dial-up terminals or terminals attached to the Internet such as TN3270 or KNET 3270 emulation), this is a **FINDING**.

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZVTM0018**

Default Severity: Category II

- a) Refer to the following item gathered from the VTAM Systems Programmer's Worksheet in the Preliminary Information Worksheets(Appendix B):
- ___ 1. A list of data set names containing all VTAM start options, configuration lists, network resource definitions, commands, procedures, exit routines, all SMP/E TLIBs, and all SMP/E DLIBs used for installation and in development/production environments.
- b) Generate a report for security verification using Analyzer.
1. Select option 4 Batch Reports from the Analyzer main menu
 2. Select option B Sensitive and Critical Data Sets Analysis
 3. Enter 'R' on line item "User defined list"
 4. Provide a dataset name or your choice which will include the names of the data sets gathered from step a) above.
Note: This may be a sequential data set or a PDS and member
 5. Specify the options as listed here.

AC(1) module list ==> NO Duplicate Module Analysis ==> NO
RACF detail ==> YES Exceptions only ==> NO
RACF Group detail ==> YES
Search criteria ==> NO
Sort criteria ==> NO
 6. Press enter to invoke the JCL Submit Processing
 7. Enter 'S' to submit the batch report
 8. Review the report for findings
- b) Ensure that RACF data set rules for all VTAM system data sets restrict access to only network systems programming staff. These data sets include libraries containing VTAM load modules and exit routines, and VTAM start options and definition statements.
- c) If (c) above is true, there is NO FINDING.
- d) If (c) above is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

WebSphere Applications Server Data Analysis

___**STIG ID: ZWAS0010**

Default Severity: Category II

- a) Generate online data set reports using Administrator for the listed data set resources.
 - 1. Option 3 Security Server Reports from the main menu
 - 2. Option 3 Data Set Profile
 - 3. Enter IMW* in the Data Set: field.
 - 4. Enter command 4 Access Lists to review the high level qualifier
 - 5. Issue the S Access List command to review access levels as required.

- b) Ensure the following data set controls are in effect for WAS:
 - 1. UPDATE and ALTER access to HTTP product data sets (i.e., hlq.IMW.AIMW** and hlq.IMW.SIMW**) is restricted to systems programming personnel.

NOTE: If the HTTP server is not used with WAS, this check can be ignored.

- 2. UPDATE and ALTER access to WAS product data sets and associated product data sets is restricted to systems programming personnel.

hlq.EJS.V3500108. (WebSphere 3.5)**

hlq.WAS.V401. (WebSphere 4.0.1)**

hlq.OE. (Java)**

hlq.JAVA (Java)**

hlq.DB2. V710107.. (DB2)**

hlq.GLD. (LDAP)**

hlq.LE. (Language Environment)**

- c) If all of the items in (b) are true, there is NO FINDING.
- d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWAS0020**

Default Severity: Category II

- a) Use Administrator option 14 Unix File Manager to determine the owner, Group, and permissions of the file system paths in the tables below. Use the XA command to expand the audit fields for verification.

Refer to the following item gathered from the IBM HTTP Server Worksheet in the Preliminary Information Worksheets:

1. DOC(IHSACCTS)

- b) The following notes apply to the requirements specified in the subsequent tables:

- If an owner field indicates **UID(0) user**, any system ID with a UID(0) specification is acceptable.
- Where an owner field indicates **websrv1**, the ID of the web server is intended.
- Where a group field indicates **webadmgl**, the ID of a local web server administration group is intended. **IMWEB** is not a valid local group.
- The site is free to set the permission and audit bit settings to be more restrictive than the documented values. Ensure the HFS permission bits, user audit bits, owner, and group for each directory and file match the specified settings listed in the following tables:

IHS VENDOR SERVER SOFTWARE HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION	USER AUDIT		OWNER	GROUP
		BITS	BITS		
/usr/lpp/internet		755	fff	UID(0) user	IMWEB
/usr/lpp/internet/bin		755	fff	UID(0) user	IMWEB
/usr/lpp/internet/sbin		750	fff	UID(0) user	IMWEB

IHS LOCAL SERVER STANDARD HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION	USER AUDIT		OWNER	GROUP
		BITS	BITS		
.../websrv1_root/		555	fff	websrv1	webadmgl
.../websrv1_root/Admin		550	fff	websrv1	webadmgl
.../websrv1_root/admin-bin		550	fff	websrv1	webadmgl
.../websrv1_root/cgi-bin		551	fff	websrv1	webadmgl
.../websrv1_root/cgi-bin		550	fff	websrv1	webadmgl
.../websrv1_root/pub	555	fff		websrv1	webadmgl

IHS LOCAL SERVER CONFIGURATION HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION	USER AUDIT		OWNER	GROUP
		BITS	BITS		
/etc/websrv1/httpd.conf		460	faf	websrv1	webadmgl
/etc/websrv1/httpd.envvars		564	faf	websrv1	webadmgl

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

/etc/websrv1/mvsds.conf	460	faf	websrv1	webadmgl
-------------------------	-----	-----	---------	----------

IHS LOCAL SERVER LOG HFS OBJECT SECURITY SETTINGS

DIRECTORY or FILE	PERMISSION	USER	AUDIT	OWNER	GROUP
		BITS	BITS		
.../websrv1_root/logs	750	fff		websrv1	webadmgl
.../websrv1_root/logs/httpd-log	750	fff		websrv1	webadmgl
.../websrv1_root/logs/httpd-errors	750	fff		websrv1	webadmgl
.../websrv1_root/logs/cgi-error	750	fff		websrv1	webadmgl

NOTE: The HFS permission bits, user audit bits, owner, and group settings specified for the WAS configuration and property files in Section 17.2.3.6 of the Z/OS STIG V4R1 is incorrect. The general guidance that was used in this section was taken from the Web Server STIG which was determined to be incorrect. Currently the STIG requires the permissions on these files to be 640, where the group is the SA or web manager account that controls the web service. However the group permission only allows READ access making it impossible to update files unless using a UID(0) account. There appears to be a conflict with this requirement.

Proposed Z/OS STIG updates include changing permissions from 640 to 460. The owner will be the web server user account and the group will be the web server administrator group. The Web Server STIG is looking into using these same settings. Verification of these proposed changes needs to be performed and the Z/OS STIG updated. Until this occurs, compliance of the WAS configuration and property files cannot be reviewed. An entry for was.conf file settings needs to be added to the STIG as well. Settings for the WebSphere properties and bin directories may be desirable.

The following represents a hierarchy for permission bits from least restrictive to most restrictive:

7	rwX(least restrictive)
6	rw-
3	-wX
2	-w-
5	r-X
4	r--
1	--X
0	---(most restrictive)

The possible audit bits settings are as follows:

f	log for failed access attempts
a	log for failed and successful access
-	no auditing

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

c) If all of the items in (b) are true, there is NO FINDING.

d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWAS0030**

Default Severity: Category II

- a) Verify the following items using Administrator:
 - 1. Option 3 Security Server Reports from the main menu.
 - 2. Option 4 General Resource Profile
 - 3. Under the Standard Masking Fields enter **CBIND** in the Class: field
 - 4. At the resulting report enter **LV** in the command area to verify access levels for item 3 below.

- b) Ensure the following items are in effect for **CBIND** resource protection:
 - 1. The **CBIND** resource class is active.
 - 2. The **CB.BIND.server_name** and **CB.server_name** resources is defined to the **CBIND** resource class with a **UACC(NONE)**.
 - 3. Access to the **CB.BIND.server_name** and **CB.server_name** resources is restricted to WAS server (STC) userids and systems management userids (e.g., WebSphere administrator ID).

- c) If all items in (b) are true, there is **NO FINDING**.

- d) If any item in (b) is untrue, this is a **FINDING**.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWAS0040**

Default Severity: Category I

- a) Create an online user report using Administrator
 - 1. Option 3 Security Server Reports
 - 2. Option 1 User Profile
 - 3. Enter **CBADMIN** on the User ID: masking field
 - 4. Enter command option 1 to generate the report
 - 5. Use the LV command to review the PWD Last Changed: information.
- b) If the **CBADMIN** user account is not defined to RACF, there is NO FINDING.
- c) If the **CBADMIN** user account is defined to RACF and the password has NOT been changed from the vendor default of **CBADMIN**, this is a FINDING with a severity code of **CAT I**.
- d) If the **CBADMIN** user account is defined to RACF and the password has been changed from the vendor default of **CBADMIN**, this is a FINDING with a severity code of **CAT II**.

CCI: CCI-001762

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___STIG ID: ZWAS0050

Default Severity: Category II

- a) Refer to the following item gathered from the IBM HTTP Server Worksheet in the Preliminary Information Worksheets:
 - 1. DOC(IHSPROCS)
- b) Review the HTTP server JCL procedure to determine the httpd.conf file to review.
- c) Ensure that all WAS-related directives are configured using the ServerInit, Service, and ServerTerm statements as outlined below.

The following path entries were added to the /etc/httpd.conf file for WebSphere 3.5:

```
ServerInit _/usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit
/usr/lpp/WebSphere/etc/WebSphere/AppServer/properties/was.conf
Service _/webapp/examples/* usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.jhtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.shtml /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/servlet/* /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service _/*.jsp /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
ServerTerm _/usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit
```

The following path entries are added to the /etc/httpd.conf file for WebSphere 4.0.1:

```
ServerInit - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:init_exit
Service - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:service_exit
ServerTerm - _/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:term_exit
```

NOTE: _The /etc/WebSphere clause for ServerInit matches the directory name above where the site customization was.conf file was established.

. Specific items to review include proper path, was.conf, and plug-in settings.

- d) If all WAS-related directives are configured properly, there is NO FINDING.
- e) If any WAS-related directive is not configured properly, this is a FINDING.

CCI: CCI-000068

CCI: CCI-000382

CCI: CCI-001762

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

MQSeries/WebSphere MQ Data Analysis

* IF MQSeries/WebSphere is not installed, this PRODUCT CAN BE SKIPPED *

___**STIG ID: ZWMQ0011**

Default Severity: Category I

- a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1      EXEC PGM=CSQUTIL, PARM='SSID'
//STEPLIB    DD DSN=CSQ700.SCSQAUTH, DISP=SHR
//           DD DSN=CSQ700.SCSQANLE, DISP=SHR
//SYSPRINT   DD SYSOUT=*
//SYSIN      DD *
COMMAND
//CSQUCMD    DD *
    DISPLAY SECURITY ALL
    DISPLAY QUEUE(*) ALL
    DISPLAY NAMELIST(*) ALL
    DISPLAY PROCESS(*) ALL
    DISPLAY CHANNEL(*) ALL
    DISPLAY QMGR DEADQ
    DISPLAY QMGR SSLKEYR
```

Below is a sample of the WebSphere MQ channel definition needed to remediate this STIG.

- b) For each WebSphere MQ channel configured to communicate with servers using WebSphere MQ, review the ssid report(s) and perform the following steps:
1. Verify that each WebSphere MQ channel is using SSL by checking for the SSLCIPH parameter, which specifies a cipher specification:

```
ECDHE_ECDSA_AES_128_CBC_SHA256
ECDHE_ECDSA_AES_256_CBC_SHA384
ECDHE_RSA_AES_128_CBC_SHA256
ECDHE_RSA_AES_256_CBC_SHA384
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
```

(Both ends of the channel must specify the same cipher specification.)
 2. Repeat these steps for *each* queue manager *ssid* identified.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- c) For each queue manager *ssid* identified, if the SSLCIPH parameter, on both sides of each WebSphere MQ channel, specifies the above in b. there is NO FINDING.
- d) If the communication lines are controlled by a VPN and are not available in the clear at any point outside the enclave, than this is acceptable and can override the requirement to use SSL. If this is true, there is NO FINDING.
- e) For each queue manager *ssid* identified , if either side of each WebSphere MQ channel specifies a cipher specification other than specified in b , **this is a FINDING unless** the communication lines are controlled by a VPN and traffic is not available in the clear at any point outside of the enclave.

For each queue manager *ssid* identified, if either side of each WebSphere MQ channel specifies a cipher specification other than DES or DES3, and the communication lines are not controlled by a VPN, this is a FINDING.

CCI: CCI-000068

CCI: CCI-002421

CCI: CCI-002423

CCI: CCI-002450

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWMQ0012**

Default Severity: Category II

- a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the “SSID” value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1      EXEC PGM=CSQUTIL, PARM='SSID'
//STEPLIB    DD DSN=CSQ700.SCSQAUTH, DISP=SHR
//           DD DSN=CSQ700.SCSQANLE, DISP=SHR
//SYSPRINT   DD SYSOUT=*
//SYSIN      DD *
COMMAND
//CSQUCMD    DD *
    DISPLAY SECURITY ALL
    DISPLAY QUEUE(*) ALL
    DISPLAY NAMELIST(*) ALL
    DISPLAY PROCESS(*) ALL
    DISPLAY CHANNEL(*) ALL
    DISPLAY QMGR DEADQ
    DISPLAY QMGR SSLKEYR
```

- b) If the site is running MQSeries 5.2 or below, this is NOT APPLICABLE.

The MQSeries release number can be found in message CSQU000I.

```
CSQU000I CSQUTIL IBM MQSeries for Z/OS - V5.2
CSQU001I CSQUTIL Queue Manager Utility - 2000-05-09 09:06:48
```

- c) For each WebSphere MQ 5.3 and above, review the *ssid* report(s) and perform these steps for *each* queue manager *ssid* identified:
- d) Review the output from step a.
- e) Verify that each WebSphere MQ 5.3 queue manager is using a digital certificate by reviewing the SSLKEYR parameter to ensure that a keyring is identified. i.e. SSLKEYR(*sslkeyring-id*)
- f) If the **SSLKEYR** parameter contains a value of **sslkeyring-id**, there is NO FINDING.
- g) If the **SSLKEYR** parameter **does not** contain a value of **sslkeyring-id**, there is a FINDING.
- h) Issue the following RACF commands, where *ssidCHIN* is the lid for the WebSphere MQ Channel Initiator’s userid and *sslkeyring-id* is obtained from the above action:

RACDCERT ID(*ssidCHIN*) LISTRING(*sslkeyring-id*)

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

NOTE: The sslkeyring-id is case sensitive.

The output will contain columns for Certificate Label Name and Cert Owner. Find the Cert Owner of ID(ssidCHIN). Use the Certificate Label Name for ID(ssidCHIN) in the following command:

```
RACDCERT ID(ssidCHIN)
LIST(LABEL('Certificate Label Name'))
```

NOTE: The Certificate Label Name is case sensitive.

Review the Issuer's Name field in the resulting output for information of any of the following:

```
OU=PKI.OU=DoD.O=U.S. Government.C=US
OU=ECA.O=U.S. Government.C=US
```

- i) Repeat these steps for *each* queue manager *ssid* identified.
- j) If OU= equals either of the above in item h) there is no finding for the OU=.

CCI: CCI-002470

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWMQ0014**

Default Severity: Category II

- a) Create a report listing the WebSphere MQ remote queues by submitting the JCL below. Add a job card and change the SSID value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1 EXEC PGM=CSQUTIL,PARM='SSID'  
//STEPLIB DD DSN=CSQ700.SCSQAUTH,DISP=SHR  
// DD DSN=CSQ700.SCSQANLE,DISP=SHR  
//SYSPRINT DD SYSOUT=*  
//SYSIN DD *  
COMMAND  
//CSQUCMD DD *  
DISPLAY QUEUE(*) TYPE(QREMOTE) ALL  
/*
```

- b) For each WebSphere MQ 5.3 and above, review the ssid report(s) and perform the following steps.

(The MQSeries release number can be found in message CSQU000I from running the CSQUTIL in step a) above.

CSQU000I CSQUTIL IBM MQSeries for Z/OS - V5.2

CSQU001I CSQUTIL Queue Manager Utility - 2000-05)

- c) From Administrator main menu, select Security Server Reports and press Enter
- d) Select General Resource Profile, option 4 and press Enter.
- e) Tab down to the Class field, enter MQQUEUE and press Enter.
- f) Find any remote queue names from the report in step a) above on the screen and enter LR next to the queue name.
- g) Press ENTER
- h) Note down all the users in the access list.
- i) List information about the certificates for each specific userid in step h) using the RACDCERT command.
- j) Verify the certificates are valid per qualifications in STIG ITNT0040.
- k) If one or more users are found with valid certificates, for each remote queue from step a) above, there is NO FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- l) If no users are found with accurate filters for any of the remote queues, this is a FINDING.
- m) If a spreadsheet is not maintained containing a list of all production Websphere MQ remote queues with associated individual USERIDS with corresponding valid Certified Name filters and reviewed annually, this is a FINDING.

CCI: CCI-000366

CCI: CCI-001133

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWMQ0020**

Default Severity: Category II

- a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the “SSID” value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1      EXEC PGM=CSQUTIL, PARM='SSID'
//STEPLIB    DD DSN=CSQ700.SCSQAUTH, DISP=SHR
//           DD DSN=CSQ700.SCSQANLE, DISP=SHR
//SYSPRINT   DD SYSOUT=*
//SYSIN      DD *
COMMAND
//CSQUCMD    DD *
    DISPLAY SECURITY ALL
    DISPLAY QUEUE(*) ALL
    DISPLAY NAMELIST(*) ALL
    DISPLAY PROCESS(*) ALL
    DISPLAY CHANNEL(*) ALL
    DISPLAY QMGR DEADQ
    DISPLAY QMGR SSLKEYR
```

- b) Review messages CSQH015I and CSQH016I:

12.36.22 STC01960 **CSQH015I** !MQ19 Security **timeout = 15 minutes**
12.36.22 STC01960 **CSQH016I** !MQ19 Security **interval = 5 minutes**

The Z/OS STIG standard value for interval is: **INTERVAL(5)**.

The Z/OS STIG standard value for timeout is: **TIMEOUT(15)**

- c) If the timeout value equals 15 minutes, there is NO FINDING.
If the interval value equals 5 minutes, there is NO FINDING.
- d) If the timeout value does not equal 15 minutes, this is a FINDING
If the interval value is not equal to 5 minutes, this is a FINDING

Repeat steps (a) thru (d) for each queue manager *ssid*.

NOTE: *ssid is the queue manager name (a.k.a., subsystem identifier).*

CCI: CCI-001133

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___**STIG ID: ZWMQ0030**

Default Severity: Category II

- a) Work with the systems programmer to identify the names of all MQSeries/WebSphere MQ started tasks.
- b) Review MQSeries/WebSphere MQ started tasks to ensure that:
 1. Each MQ started task (ssidMSTR and ssidCHIN) is associated with a **unique** userid.
 2. All MQ started tasks (ssidMSTR and ssidCHIN) are defined to the **STARTED** resource class.
 3. All MQ started tasks (ssidMSTR and ssidCHIN) userid are defined as a **PROTECTED**.

Using Vanguard Analyzer:

1. From the main Menu, select 3 (Online Displays), press <ENTER>.
2. Select 4 (Started Procedures Analysis) and press <ENTER>.

Review the **Procname** and **USERID** columns associated with each MQSeries/WebSphere MQ started task identified in step a).

Using Vanguard Administrator:

1. From the main menu, type **3** (Security Server Reports), press <ENTER>.
 2. Type **1** (User Profiles), press <Enter>.
 3. Tab down to the PROTECTED field, type Y and press <ENTER>.
 4. All PROTECTED userids will be displayed.
- b) For each MQ started task name, if the userid contained in the **Userid** column of the Analyzer report is unique (i.e. is not associated with any other started task name), there is NO FINDING.
 - c) If the name of each MQ started task is displayed in the Procname column of the Analyzer report (e.g. defined to the STARTED resource class), there is NO FINDING.
 - d) Using the Administrator “Protected Userid Report”, if all MQ started tasks (identified in the Analyzer report) appear in the Userid column, there is NO FINDING.
 - e) For each MQ started task name, if the userid contained in the **Userid** column of the Analyzer report is not unique (i.e. is associated with other started task names), this is a FINDING
 - f) If the name of any MQ started task is not displayed in the Procname column of the Analyzer report (e.g. not defined to the STARTED resource class), this is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- g) Using the Administrator “Protected Userid Report”, if a MQ started task userid (identified in the Analyzer report) does not appear in the Userid column, this is a FINDING

CCI: CCI-000764

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0040**

Default Severity: Category II

- a) Consult with the MQSeries systems programmer to identify the names of the MQSeries system data sets, log data sets and archive datasets that protect MQSeries data.
- b) Ensure RACF data sets rules for MQSeries/WebSphere MQ system data sets (e.g., SYS2.MQM.***) restrict access as follows:

___ READ access to data sets referenced by the following DDnames is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel. All access to these data sets is logged.

<u>DDname</u>	<u>Procedure</u>	<u>Description</u>
CSQINP1	ssidMSTR	Input parameters
CSQINP2	ssidMSTR	Input parameters
CSQXLIB	ssidCHIN	User exit library

NOTE: UPDATE and/or ALTER access to these data sets is restricted to MQSeries/WebSphere

Using Administrator:

1. From the main menu, go to the **Dataset Profile Reports** menu by typing **3;3** and press <ENTER>.
2. Tab down to the Data Set row and over-type the * with the names of each dataset identified in step a).
3. Review the universal access, access list and audit attributes for each profile that protects datasets identified in step a).

For dataset profiles that protect resources identified in the above DDname statements:

1. If MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel have **READ** access, there is NO FINDING.
2. If MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and system programming personnel have UPDATE and/or ALTER access, there is a FINDING.
3. If audit **ALL(READ)** is specified, there is NO FINDING

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

4. If audit **ALL(READ)** is not specified, there is a FINDING.

____ UPDATE and/or ALTER access to data sets referenced by the following DDnames is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, and systems programming personnel. All UPDATE and ALTER access to these data sets is logged.

<u>DDname</u>	<u>Procedure</u>	<u>Description</u>
CSQPxxxx	ssidMSTR	Page data sets
BSDSx	ssidMSTR	Bootstrap data sets
CSQOUTx	ssidMSTR	SYSOUT data sets
CSQSNAP	ssidMSTR	DUMP data set
(See note)	ssidMSTR	Log data sets

NOTE: To determine the log data set names, review the **JESMSG LG** file of the **ssidMSTR** active task(s). Find **CSQJ001I** messages to obtain DSNs.

For dataset profiles that protect resources identified in the above DDname statements:

5. If MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators and system programming personnel have UPDATE and/or ALTER access, there is NO FINDING.
6. If any users other than MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators and system programming personnel have an access level greater than UPDATE, there is a FINDING.
7. If all UPDATE and ALTER access to these datasets is being logged, there is NO FINDING
8. If all UPDATE and ALTER access to these datasets is not being logged, there is a FINDING.

____ ALTER access to **archive data sets** is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel. All ALTER access to these data sets is logged.

NOTE: To determine the archive data sets names, review the **JESMSG LG** file of the **ssidMSTR** active task(s). Find the **CSQY122I** message to obtain the **ARCPRFX1** and **ARCPRFX2** DSN HLQs.

9. If ALTER access to archive data sets is restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel, there is NO FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

10. If ALTER access to archive data sets is not restricted to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrator, and system programming personnel, there is a FINDING.
 11. If all ALTER accesses to archive data sets is being logged, there is NO FINDING.
 12. If all ALTER access to archive data sets is not being logged, there is a FINDING.
 13. **Except for the specific data set requirements just mentioned**, if UPDATE and/or ALTER access to all other MQSeries/WebSphere MQ system datasets is restricted to the MQSeries/WebSphere MQ administrator and systems programming personnel, there is NO FINDING.
 14. **Except for the specific data set requirements just mentioned**, if UPDATE and/or ALTER access to all other MQSeries/WebSphere MQ system datasets is not restricted to the MQSeries/WebSphere MQ administrator and systems programming personnel, there is a FINDING.
- c) If all the items in (b) are true, there is NO FINDING.
- d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-000213

CCI: CCI-001499

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0049**

Default Severity: Category II

a) Use Analyzer to display active classes.

1. From the Analyzer main Menu, select 3 (Online Displays), press <ENTER>
2. Select 7 (SETROPTS Analysis) and press <ENTER>
3. Tab down and type an **S** next to “Audit for CDT Classes”, press <ENTER>
4. Resource class names are displayed in the Class column, the status of each resource class name (inactive/active) is displayed in the Status column.
5. Press PF8 to find each class name documented in b) below.

b) Ensure that the following MQ Series resource classes are active below V 7.0.0:

MQADMIN
GMQADMIN
MQCONN
MQCMDS
MQQUEUE
GMQQUEUE
MQPROC
GMQPROC
MQNLIST
GMQNLIST

NOTE: If the **MQADMIN** resource class is not active, **no** security checking is performed.

For V7.0.0 and above these classes must be active:

GMXADMIN
GMXNLIST
GMXPROC
GMXQUEUE
GMXTOPIC
MXADMIN
MXNLIST
MXPROC
MXQUEUE
MXTOPIC

c) If all of the resource classes above are ACTIVE (e.g. “active” is displayed in the status column), there is NO FINDING.

d) If any resource classes above are INACTIVE (e.g. “inactive” is displayed in

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

the status column), this is a FINDING.

CCI: CCI-000213

CCI: CCI-002358

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0051**

Default Severity: Category I

- a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the “SSID” value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1      EXEC PGM=CSQUTIL, PARM='SSID'
//STEPLIB    DD DSN=CSQ700.SCSQAUTH, DISP=SHR
//           DD DSN=CSQ700.SCSQANLE, DISP=SHR
//SYSPRINT   DD SYSOUT=*
//SYSIN      DD *
COMMAND
//CSQUCMD    DD *
    DISPLAY SECURITY ALL
    DISPLAY QUEUE(*) ALL
    DISPLAY NAMELIST(*) ALL
    DISPLAY PROCESS(*) ALL
    DISPLAY CHANNEL(*) ALL
    DISPLAY QMGR DEADQ
    DISPLAY QMGR SSLKEYR
```

- b) Review the Security switches. If all of the following switches specify **ON**, there is **NO FINDING**.

SUBSYSTEM	CONNECTION	COMMAND	CONTEXT	ALTERNATE USER
PROCESS	NAMELIST	QUEUE	COMMAND	RESOURCES

For example:

```
10.05.01 STC01960 CSQH030I !MQ19 Security switches ...
10.05.01 STC01960 CSQH034I !MQ19 SUBSYSTEM: ON,
10.05.01 STC01960 CSQH031I !MQ19 CONNECTION: ON,
10.05.01 STC01960 CSQH034I !MQ19 COMMAND: ON,
10.05.01 STC01960 CSQH031I !MQ19 CONTEXT: ON,
10.05.01 STC01960 CSQH034I !MQ19 ALTERNATE USER: ON,
10.05.01 STC01960 CSQH034I !MQ19 PROCESS: ON,
10.05.01 STC01960 CSQH034I !MQ19 NAMELIST: ON,
10.05.01 STC01960 CSQH034I !MQ19 QUEUE: ON,
10.05.01 STC01960 CSQH031I !MQ19 COMMAND RESOURCES: ON,
```

- c) If the SUBSYSTEM switch is OFF, **this is a FINDING with a severity of Category I.**
- d) If any of the other above switches specify **OFF** (other than the exception mentioned below), **this is a FINDING, downgrade the severity to a Category II.**

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

- e) If the **COMMAND RESOURCE** Security switch specifies **OFF**, there is NO FINDING.

***NOTE:** At the discretion of the IAO, **COMMAND RESOURCE** Security switch may specify **OFF**, by defining **ssid.NO.CMD.RESC.CHECKS** in the MQADMIN resource class.*

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0052**

Default Severity: Category II

a) Using Administrator:

1. From the Administrator main menu, select 3 (Security Server Reports) and press <ENTER>
2. From the SECURITY SERVER REPORTS, select 4 (General Resource Reports) and press <ENTER>
3. Tab down to "CLASS: ", type MQCONN and press <ENTER>
4. For each profile in b) below, type **LR** in the CMD column of each displayed profile to review the corresponding UACC column, access list and audit attributes.

b) Review the following connection resources defined to the MQCONN resource class:

<u>Resource</u>	<u>Authorized Users</u>
ssid.BATCH	TSO and batch job userids
ssid.CICS	CICS region userids
ssid.IMS	IMS region userids
ssid.CHIN	Channel initiator userids

***NOTE:** ssid is the queue manager name (a.k.a., subsystem identifier).*

c) For all connection resources defined to the **MQCONN** resource class, ensure the following items are in effect:

***NOTE:** If you do **not** have a resource profile defined for a particular security check, and a user issues a request that would involve making that check, MQSeries/WebSphere MQ denies access.*

1. If all UACC's are equal to NONE, there is NO FINDING.
2. If access authorization to each profile restricts access to the appropriate users as indicated in b) above, there is NO FINDING.
3. If all access is logged, (e.g. **ALL(READ)**), there is NO FINDING

d) For all connection resources defined to the **MQCONN** resource class,

1. If any UACC is not equal to NONE, this is a FINDING
2. If access authorization to any profile includes inappropriate users that are not listed above, there is a FINDING.
3. If all access is not logged, (e.g. not **ALL(READ)**), this is a FINDING

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0053**

Default Severity: Category II

- a) Create a report showing the WebSphere MQ channel definitions by submitting the JCL below. Add a job card and change the “SSID” value in the EXEC statement to your MQ SSID.

Note: This job must be run for each SSID.

```
//STEP1      EXEC PGM=CSQUTIL, PARM='SSID'
//STEPLIB    DD DSN=CSQ700.SCSQAUTH, DISP=SHR
//           DD DSN=CSQ700.SCSQANLE, DISP=SHR
//SYSPRINT   DD SYSOUT=*
//SYSIN      DD *
COMMAND
//CSQUCMD    DD *
  DISPLAY SECURITY ALL
  DISPLAY QUEUE(*) ALL
  DISPLAY NAMELIST(*) ALL
  DISPLAY PROCESS(*) ALL
  DISPLAY CHANNEL(*) ALL
  DISPLAY QMGR DEADQ
  DISPLAY QMGR SSLKEYR
```

b)

1. Locate the start of the dead-letter queue information. Review the **DEADQ** parameter to obtain the name of the *real* dead-letter queue.
2. Find the **QUEUE(*dead-letter.queue.name*)** entry to locate the start of the *real* dead-letter queue definition. Review the **GET** and **PUT** parameters to determine their values, and ensure they conform to those specified in the **Z/OS STIG**.

The **Z/OS STIG** standard values are:

GET (ENABLED)
PUT (ENABLED)

NOTE: *Dead-letter.queue.name* is the value of the **DEADQ** parameter determined in Step 1.

- 2.1 If GET(ENABLED) and PUT(ENABLED) are specified, there is NO FINDING.
 - 2.2 If GET(ENABLED) and PUT(ENABLED) are not specified, there is a FINDING.
3. From the top of the report, find the **QUEUE(*dead-letter.queue.name*.PUT)** entry to locate the start of the *alias* dead-letter

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

queue definition.

Review the GET and PUT parameters to determine their values, and ensure they conform to those specified in the **Z/OS STIG**.

The **Z/OS STIG** standard values are:

GET (DISABLED)
PUT (ENABLED)

Note 1: *Dead-letter.queue.name* is the value of the **DEADQ** parameter determined in Step 1.

Note 2: The **TARGQ** parameter value for the alias queue will be the real dead-letter queue name.

Note 3: If an alias queue is not used in place of the dead-letter queue, then the **RACF** rules for the dead-letter queue must be coded to restrict unauthorized users and systems from reading the messages on the file.

- 3.1 If GET(DISABLED) and PUT(ENABLED) are specified, there is NO FINDING.
- 3.2 If GET(DISABLED) and PUT(ENABLED) are not, there is a FINDING.

4) Repeat these steps for *each* queue manager *ssid*.

- c) If all of the items in (b) are true, there is NO FINDING.
- d) If any item in (b) is untrue, this is a FINDING.

CCI: CCI-001762

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0054**

Default Severity: *Category II*

- a) Use Administrator to analyze all profiles in the **MQQUEUE** and **GMQUEUE** resource classes.
 1. From the Administrator main menu, type **3** on the command line (Security Server Reports) and press <ENTER>.
 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 3. Tab down to “CLASS: ”, type **MQQUEUE** or **GMQUEUE**, as appropriate, and press <ENTER>.

NOTE: *ssid* is the queue manager name (a.k.a., subsystem identifier).

- b) For all queue resources defined to the **MQQUEUE** or **GMQUEUE** resource classes, ensure the following items are in effect.
 1. Resource profiles are defined with a **UACC(NONE)**
 - a. If all UACC's are equal to NONE, there is NO FINDING.
 - b. If any UACC is not equal to NONE, there is a FINDING.
 2. For message queues (i.e., *ssid.queueuname*), access authorization restricts access to users requiring the ability to get messages from and put messages to message queues. This is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.
 - a. If access authorization restricts access to users requiring the ability to get messages from and put messages to message queues, there is NO FINDING.
 - b. If access authorization allows access to users who do not require the ability to get messages from and put messages to message queues, there is a FINDING
 3. For the system queues (i.e., *ssid.SYSTEM.queueuname*), ALTER access authorization restricts access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, systems programming personnel, and CICS regions running MQSeries/WebSphere MQ applications.
 - a. If ALTER access authorization restricts access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, systems programming personnel, and CICS regions running MQSeries/WebSphere MQ applications, there is NO

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

FINDING.

- b. If ALTER access authorization does not restrict access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, systems programming personnel, and CICS regions running MQSeries/WebSphere MQ applications, there is a FINDING.
4. For the following system queues ensure that type **LR** in the CMD column next to them and ensure UPDATE access is restricted to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require access to review message queues.

ssid.SYSTEM.COMMAND.INPUT
ssid.SYSTEM.COMMAND.REPLY
ssid.SYSTEM.CSQOREXX.*

- a. If the above System queues have update access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require access to review message queues, there is NO FINDING.
 - b. If the above System queues DO NOT have update access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, auditors, and users that require access to review message queues, there is a FINDING.
5. For system queues (i.e., ssid.SYSTEM.CSQUTIL.*) ensure that UPDATE access is restricted to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors.
- a. If the system queues (i.e., ssid.SYSTEM.CSQUTIL.*) have UPDATE access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors, there is NO FINDING.
 - b. If the system queues (i.e., ssid.SYSTEM.CSQUTIL.*) DO NOT have UPDATE access limited to WebSphere MQ STCs, WebSphere MQ administrators, systems programming personnel, CICS regions running WebSphere MQ applications, and auditors, there is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

6. Type **LR** in the CMD column of the *real* dead-letter queue (refer to **STIG ID ZWMQ0053**). Review the access list for the displayed profile.
 - a. If access restricts access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, CICS regions running MQSeries/WebSphere MQ applications, and any automated application used for dead-letter queue maintenance, there is **NO FINDING2**.
 - b. If access authorization does not restrict access to MQSeries/WebSphere MQ STCs, MQSeries/WebSphere MQ administrators, CICS regions running MQSeries/WebSphere MQ applications, and any automated application used for dead-letter queue maintenance, there is a **FINDING**.
7. Type **LR** in the CMD column of the *alias* dead-letter queue (refer to **STIG ID ZWMQ0053**). Review the access list for the displayed profile.
 - a. If access authorization restricts access to users requiring the ability to put messages to the dead-letter queue, there is **NO FINDING**.
 - b. If access authorization does not restrict access to users requiring the ability to put messages to the dead-letter queue, there is a **FINDING**
8. Repeat steps a thru b for each profile in the **GMQUEUE** class.
 - c) If all of the items in B were identified as **NO FINDING**, there is **NO FINDING**.
 - d) If any of the items in B were identified as a **FINDING**, there is a **FINDING**.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0055**

Default Severity: Category II

- a) Use Administrator to analyze all process name resource profiles in the **MQPROC** and **GMQPROC** resource classes.
 1. From the Administrator main menu, type **3** on the command line (Security Server Reports) and press <ENTER>.
 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 3. Tab down to "CLASS: ", type **MQPROC**, and press <ENTER>.
 4. For all process name profiles displayed (i.e., *ssid.processname*) in the "Profile Name" column, review the corresponding UACC column.

***NOTE:** **ssid** is the queue manager name (a.k.a., subsystem identifier).*

- b) For all process resources (i.e., *ssid.processname*) defined to the **MQPROC** or **GMQPROC** resource classes, ensure the following items are in effect:

***NOTE 1:** **ssid** is the queue manager name (a.k.a., subsystem identifier).*

1. Resource profiles are defined with a **UACC(NONE)**
 - a. If all UACC's are equal to NONE, there is NO FINDING
 - b. If any UACC is not equal to NONE, there is a FINDING

Type **LR** in the CMD column of each profile. Review the access list for each displayed profile.

2. Restrict access to users requiring the ability to make process inquiries.

***Note:** Identifying users authorized to make process inquiries is difficult to determine. However, an item for concern may be a profile with * READ specified in the access list.*

- a. If access authorization restricts access to users requiring the ability to make process inquiries, there is NO FINDING.
- b. If access authorization allows access to users who do not require the ability to make process inquiries, there is a FINDING

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

Repeat steps (a) thru (b) for each profile in the **GMQPROC** class.

- c) If all of the items in B were identified as NO FINDING, there is NO FINDING.
- d) If any of the items in B were identified as a FINDING, there is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0056**

Default Severity: Category II

- a) Use Administrator to analyze all namelist resource profiles in the **MQNLIST** and **GMQNLIST** resource classes.
 - 1. From the Administrator main menu, type **3** on the command line (Security Server Reports) and press <ENTER>.
 - 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 - 3. Tab down to “CLASS: ”, type **MQNLIST**, and press <ENTER>.
 - 4. For all profiles displayed in the “Profile Name” column, review the corresponding UACC column.

***NOTE:** ssid is the queue manager name (a.k.a., subsystem identifier).*

- b) For all namelist resources (i.e., *ssid.namelist*) defined to the **MQNLIST** or **GMQNLIST** resource classes, ensure the following items are in effect:

***NOTE 1:** ssid is the queue manager name (a.k.a., subsystem identifier).*

- 1. Resource profiles are defined with a **UACC(NONE)**
 - a. If all UACC's are equal to NONE, there is NO FINDING
 - b. If any UACC is not equal to NONE, there is a FINDING

Type **LR** in the CMD column of each profile. Review the access list for each displayed profile.

- 2. Restrict access to users requiring the ability to make namelist inquiries.

***Note:** Identifying users authorized to make namelist inquiries is difficult to determine. However, an item for concern may be a profile with *READ specified in the access list.*

- a. If access authorization restricts access to users requiring the ability to make namelist inquiries, there is NO FINDING2.
- b. If access authorization allows access to users who do not require the ability to make namelist inquiries, there is a FINDING.

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

Repeat steps (a) thru (b) for the **GMQNLIST** class.

- c) If all of the items in B were identified as NO FINDING, there is NO FINDING.
- d) If any of the items in B were identified as a FINDING, there is a FINDING.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0057**

Default Severity: Category II

- a) Use Administrator to analyze all alternative resource profiles in the **MQADMIN** resource classes.
 - 1. From the Administrator main menu, type **3** on the command line (Security Server Reports) and press <ENTER>.
 - 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 - 3. Tab down to “CLASS: ”, type **MQADMIN** and press <ENTER>
 - 4. For all alternate user resources (i.e. *ssid.ALTERNATE.USER.alternateuserid*) displayed in the “Profile Name” column, review the corresponding UACC column
 - 5. Type **LR** in the CMD column of each alternate user resource (i.e. *ssid.ALTERNATE.USER.alternateuserid*). Review the access list for each displayed profile.
- b) For all alternate user resources (i.e., *ssid.ALTERNATE.USER.alternateuserid*) defined to the **MQADMIN** resource class, ensure the following items are in effect:

***NOTE:** ssid is the queue manager name (a.k.a., subsystem identifier).*

- 1. Resource profiles are defined with a **UACC(NONE)**.
 - 2. Access authorization restricts access to users requiring the ability to use the alternate userid. This is difficult to determine. However, an item for concern may be a profile with * **READ** specified in the access list.
- c) If both of the items in (b) are true, there is **NO FINDING**.
- d) If either item in (b) is untrue, this is a **FINDING**.

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0058**

Default Severity: Category II

- a) Use Administrator to analyze all context resource profiles in the **MQADMIN** resource class.
 1. From the Administrator main menu, select 3 (Security Server Reports) and press <ENTER>.
 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 3. Tab down to "CLASS: ", type **MQADMIN** and press <ENTER>.
 4. For all context resources (i.e., *ssid.CONTEXT*) displayed in the "Profile Name" column, review the corresponding UACC column.
 5. Type **LR** in the CMD column of each context resource profile (i.e., *ssid.CONTEXT*). Review the access list for each displayed profile.
- b) For all context resources defined to the **MQADMIN** resource classes, ensure the following items are in effect.

NOTE: *ssid* is the queue manager name (a.k.a., subsystem identifier).

Access authorization restricts access to users requiring the ability to pass or set identity and/or origin data for a message. This is difficult to determine. However, an item for concern may be a profile with * **READ** specified in the access list.

1. If all UACC's are equal to NONE, there is NO FINDING.
2. If any UACC is not equal to NONE, there is a FINDING.
3. If access authorization restricts access to users authorized to use the alternate userid, there is NO FINDING
4. If access authorization allows users who are not authorized to use the alternate userid, there is a FINDING

CCI: CCI-000213

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0059**

Default Severity: Category II

- a) Use Administrator to analyze all command resource profiles (i.e., *ssid.command*) in the **MQCMDS** resource class.
1. From the Administrator main menu, select 3 (Security Server Reports) and press <ENTER>.
 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 3. Tab down to "CLASS: ", type **MQCMDS** and press <ENTER>.
 4. For all command resource profiles (i.e., *ssid.command*) displayed in the "Profile Name" column, review the corresponding UACC column.
 5. Type **LR** in the CMD column of each command resource profile (i.e., *ssid.command*). Review the access list and audit attributes for each displayed profile.

***NOTE:** *ssid* is the queue manager name (a.k.a., subsystem identifier).*

- b) For all command resources (i.e., *ssid.command*) defined to the **MQCMDS** resource class, ensure the following items are in effect:
1. Review the universal access for each displayed profile.
 - a. If all UACC's are equal to NONE, there is NO FINDING.
 - b. If any UACC is not equal to NONE, there is a FINDING.
 2. Review the audit attributes for each displayed profile.
 - a. If all command access is logged as designated in the table entitled Command Security Controls in Section 4.3.4.2.9, (MQSeries/WebSphere MQ) Command Security, of the **Z/OS STIG**, there is NO FINDING
 - b. If all command access is not logged as designated in the table below this is a FINDING
 3. Review the access list for each displayed profile.
 - a. If access authorization is restricted to appropriate personnel as designated in the table entitled Command Security Controls in in the U_zOS_STIG_Addendum, there is NO FINDING.
 - b. If access authorization is not restricted to appropriate personnel as designated in the table entitled Command Security Controls in in the U_zOS_STIG_Addendum, there is a FINDING.

- c) If all of the items in (b) were identified as NO FINDING, there is NO

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

FINDING.

If any of the items in (b) were identified as a FINDING, there is a FINDING.

CCI: CCI-000213

CCI: CCI-002234

UNCLASSIFIED
z/OS RACF Analysis and Checklist
Version 6 Release 39

___ **STIG ID: ZWMQ0060**

Default Severity: Category II

- a) Use Administrator to analyze all RESLEVEL resource profiles (i.e., *ssid.RESLEVEL*) in the **MQCMDS** resource class.
 - 1. From the Administrator main menu, select 3 (Security Server Reports) and press <ENTER>.
 - 2. Type **4** on the command line (General Resource Reports) and press <ENTER>.
 - 3. Tab down to “CLASS: ”, type **MQCMDS** and press <ENTER>.
 - 4. For all RESLEVEL resource profiles (i.e., *ssid.RESLEVEL*) displayed in the “Profile Name” column, review the corresponding UACC column.
 - 5. Type **LR** in the CMD column of each RESLEVEL resource profile, review the access list.
- b) Ensure that the following items are in effect:

NOTE: *ssid* is the queue manager name (a.k.a., subsystem identifier).

- 1. For all RESLEVEL resource profiles, review the corresponding UACC column.
 - a. If all UACC’s are equal to NONE, there is NO FINDING
 - b. If any UACC is not equal to NONE, there is a FINDING
- 2. For all RESLEVEL resource profiles, review the corresponding UACC column.
 - a. If no users or groups are specified on the access list, there is NO FINDING
 - b. If any users or groups are specified on the access list this is a FINDING
- c) If all of the items in (b) were identified as NO FINDING, there is NO FINDING.
- d) If any of the items in (b) were identified as a FINDING, there is a FINDING.

CCI: CCI-000213

CCI: CCI-001762