RACF AUDIT GUIDANCE

January 2017

INTRODUCTION: Since it was first introduced in 1976, RACF's security capabilities along with those of the IBM mainframe operating system (currently known as z/OS) have been progressively enhanced. New control features and functionality have been added while earlier control options are rarely used or have become obsolete altogether. The purpose of this document is to inform RACF auditors of some control options and issues that may no longer be of significant concern nor merit an audit finding. (Auditors who are unfamiliar with RACF are encouraged to first read RSH's "RACF - An Overview" before reading further.)

SETROPTS JES(EARLYVERIFY): JES (Job Entry Subsystem) is the system task that manages the execution of batch jobs. There are two variations of JES - JES2 and JES3. In releases of JES prior to 3.1.3 (before 1990), verification of a USERID and password coded on the JOB statement of a batch job was not done until the job was executed. This could occur quite some time after the job was initially submitted. While the job waited for execution, the job, including its unencrypted password was stored in JES. Someone could use special software tools to scan JES files and discover the password. To address this concern, RACF introduced SETROPTS option JES(EARLYVERIFY) to force the password to be verified and discarded at job submission time. Beginning with JES release 3.1.3, this early verification process became automatic. The JES(EARLYVERIFY) option is now meaningless, and its status, if inactive, should not trigger an audit finding. (Reference: z/OS Security Server RACF Security Administrator's Guide)

SETROPTS JES(XBMALLRACF) & EXECUTION BATCH MONITORS (XBM): All batch jobs entering the system should have an associated RACF ID. The RACF SETROPTS option JES(BATCHALLRACF) enforces this for normal batch jobs, and it should be active. Option JES(XBMALLRACF) only applies to JES2 and only to jobs managed by Execution Batch Monitors (XBMs). Use of XBMs is now exceedingly rare. The existence of an XBM is determined by examining the initialization parameters associated with JES2 (a.k.a. JESPARMS). If the keyword XBM=*procedure-name* is not coded on any JOBCLASS statement, no XBMs are being used, and SETROPTS JES(XBMALLRACF) need not be active. It is acceptable to encourage the auditee to activate it simply for completeness and consistency; however, if XBMs are not being used, no audit finding should be issued if this option is inactive. (Reference: z/OS JES2 Initialization and Tuning Reference)

SETROPTS ADSP (AUTOMATIC DATASET PROTECTION): Prior to the introduction of Generic profiles in the mid-1980s, it was necessary to define a Discrete profile for each individual dataset in order to protect it. It was burdensome to have to manually define a profile for each new dataset, so the ADSP option was introduced to ensure Discrete profiles were automatically defined. When SETROPTS ADSP is active and a user has the ADSP attribute, RACF creates a Discrete profile for every dataset the user creates. Today, most datasets are protected by Generic profiles which are much easier to administer. The use of Discrete profiles is generally avoided. Hence, it is acceptable, even desirable, for option ADSP to be turned off. In fact, IBM recommends it be deactivated. (Reference: z/OS Security Server RACF Security Administrator's Guide)

PROGRAM AMASPZAP (SUPERZAP): Program AMASPZAP and its alias IMASPZAP, commonly known as SUPERZAP or SPZAP, is a service aid utility that can be used to fix a program load module or correct a Direct Access Storage Device (DASD) Volume Table of Contents (VTOC) entry at the individual bit level. Originally, it would make such changes without checking for RACF authorization. This was a significant security concern back in the days when the only means of protecting a dataset was with a Discrete profile. When a Discrete profile is created, RACF turns on the RACF-Indicated bit in the dataset's VTOC entry. This tells the system to check RACF for a Discrete profile. SUPERZAP could turn the bit off and fool the system into thinking the dataset was unprotected. This made the protection and control of SUPERZAP a major issue. This is no longer the case. SUPERZAP now runs in 'Problem" state (as opposed to "Supervisor" or "Privileged" state), and its use is subject to normal RACF controls. To change a program, the user must have at least UPDATE access to the library where the target program resides. To update a VTOC, the user must have at least UPDATE access to the DASDVOL or GDASDVOL profile guarding the DASD volume and a computer operator must respond affirmatively to a console message requesting permission to perform the action. Besides, in today's RACF environments, datasets are very rarely protected by Discrete profiles. They

RACF is a Trademark of the International Business Machines Corporation

are instead protected by Generic profiles which use wild-card masking characters to protect multiple datasets. If you find a Discrete profile, it was probably created by mistake. Furthermore, if someone were to turn off the RACF-indicated bit on a dataset protected by a Discrete profile, RACF would simply use the closest matching Generic profile to protect the dataset. Taking all this into consideration, it is no longer a necessity to restrict the use of SUPERZAP. (Reference: z/OS MVS Diagnosis: Tools and Service Aids)

IBMUSER: IBMUSER is the default USERID created when a RACF database is initialized. It is intended to be used only when RACF is first installed to create the first few IDs with SPECIAL authority (i.e., Security Administrator IDs) and is then to be REVOKED (i.e., deactivated) immediately thereafter. Installations are encouraged to further limit the capabilities of this ID by removing its SPECIAL and OPERATIONS authority, making it RESTRICTED and PROTECTED, and assigning it a null Unix UID. This ID, however, should not be deleted. If, during database initialization, RACF cannot find IBMUSER, RACF will automatically recreate it. The recreated IBMUSER will have all of its powerful authorities, it will not be REVOKED, and it will be assigned its original, well-known default password, making it open for misuse by anyone who knows the default password. (Reference: z/OS Security Server RACF Security Administrator's Guide)

PROGRAM PROPERTIES TABLE (PPT): The PPT is used to assign special authorities to specific programs executed from Authorized Program Facility (APF) libraries. Programs in APF libraries should be regarded as extensions of the operation system with all its inherent powers. Two PPT authorities of particular interest are KEY(n) and NOPASS. KEY(n), where 'n' is 0 through 7, enables a program to execute with a System Key which allows access to operating system software in memory and the use of privileged Supervisor Calls (SVCs). NOPASS (Bypass Password Protection) allows a program to access any dataset without requiring a dataset password (an ancient, obsolete form of protection) or RACF authorization. There is a substantial set of PPT entries that come standard with the operating system, and many have one or both of these authorities. Installations can add their own entries by defining them in a system parameter library (a.k.a. PARMLIB) in members named SCHEDxx, where 'xx' is a two-character suffix. The SCHEDxx member(s) loaded at IPL can be dynamically replaced any time thereafter with an operator SET command. The SYSPPT report generated by the RACF DSMON utility provides a listing of the current PPT in an individual z/OS system. The IBM-provided entries include programs that may not be applicable to every system. For example, most installations use JES2, yet the PPT has an entry for program IATINTK, which is only used by JES3. There is no harm in having these dormant entries in the PPT, and removing them does not eliminate any security exposures. Any user with UPDATE or greater access to an APF-authorized library could misuse any PPT entry, dormant or not, simply by creating and executing an identically-named program. Restricting UPDATE access to APF-authorized libraries is the only meaningful form of protection. (Reference: z/OS MVS Initialization and Tuning Reference)

Program modifications introduced with Security APAR (Authorized Program Analysis Report) OA50215, released in June 2016, changed the behavior of NOPASS. After applying the APAR, NOPASS will enable a program to bypass RACF dataset protection only when it is executed as a Started Task. New parameter NOPASS_ALLOWBATCH can be specified to allow a program to bypass protection in batch. IBM has stated that the use of this new parameter may open integrity issues and is best avoided.

BUILT-IN IRR-PREFIXED DIGITAL CERTIFICATE IDS: Three USERIDs are installed in RACF to support digital certificates. They are irrcerta (CERTAUTH Anchor), irrmulti (Criteria Anchor), and irrsitec (SITE Anchor). The IDs are revoked and cannot be used for logon or any other purpose. They appear to be inactive. These IDs must not be deleted. If, during database initialization, RACF cannot find these IDs, RACF will automatically recreate them. (Reference: z/OS Security Server RACF Security Administrator's Guide)

Contact RSH Consulting for training or assistance with auditing RACF.