INTRODUCTION: Since it was first introduced in 1976, RACF's security capabilities along with those of the IBM mainframe operating system z/OS have been progressively enhanced. New control features and functionality have been added while some older control options are now to be avoided 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. (JES3 is no longer offered by IBM but can be licensed from Phoenix Software as JES3Plus.) In releases of JES prior to 3.1.3 (circa 1988), verification of a USERID and password coded on the JOB statement of a batch job was not performed until the job was executed. This could occur quite some time after the job was initially submitted. While awaiting execution, the job and its unencrypted password were stored in JES. Someone with specialized software tools could scan JES files and discover the password. To address this concern, RACF introduced SETROPTS option JES(EARLYVERIFY) to force the password to be immediately 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): Ideally, all batch jobs entering the system should have an associated RACF ID. 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's HASPPARMs. 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. Even 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, is a service aid utility that can be used to make changes at the individual bit level to fix a program load module or correct a Direct Access Storage Device (DASD) Volume Table of Contents (VTOC) entry. Originally, it was empowered to make such changes without requiring any RACF authorization. This was a significant security concern back in the days when the only means of protecting datasets was with Discrete profiles. A dataset's VTOC entry contains a RACF-Indicated bit. This bit is turned on when a Discrete profile is created for a dataset, and it prompts the system to check the Discrete profile for access authorization. SUPERZAP could turn the bit off and fool the system into thinking the dataset was unprotected. This functionality made the protection and control of SUPERZAP a necessity. This is no longer

the case. SUPERZAP now runs in 'Problem" state (as opposed to "Supervisor" or "Privileged" state). To modify program code, the user must now have UPDATE access to the library dataset where the target program resides. To update a VTOC, the user must have 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. Furthermore, datasets nowadays are very rarely protected by Discrete profiles. If you find a Discrete profile, it was probably created by mistake. Most datasets are now protected by Generic profiles. Generic profiles typically use wild-card masking characters to protect multiple datasets. Generic profile use is unaffected by the RACF-Indicated bit setting. 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 essential to restrict the use of SUPERZAP. (Reference: z/OS MVS Diagnosis: Tools and Service Aids)

IBMUSER: IBMUSER is the default USERID defined when a RACF database is first initialized. It is intended to be used only to create the first few IDs with SPECIAL authority (i.e., Security Administrator IDs). Once these IDs have been created, IBMUSER should be REVOKED (i.e., deactivated) and never used again. In addition to making the ID REVOKED, installations are strongly encouraged to remove its SPECIAL, OPERATIONS, and AUDITOR authorities, make it RESTRICTED and PROTECTED, add the UAUDIT attribute, set REVOKE and AUTHORITY(USE) on its connection to group SYS1, and assign it a null z/OS Unix UID. This ID should not be deleted. If RACF cannot find IBMUSER during database initialization at system start-up, RACF will automatically recreate it. The recreated IBMUSER will have all of its powerful default authorities, it will not be REVOKED, and it will be assigned its original, well-known default password, exposing it to 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 operating 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 old, obsolete form of protection) or RACF authorization. z/OS has an IBM-provided PPT containing about one hundred entries, and many have one or both of these authorities. Installations can add their own entries by defining them in system configuration parameter libraries (a.k.a. PARMLIBs) 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. Any installation added entries with either of these attributes should be scrutinized. The SYSPPT report generated by the RACF DSMON utility provides a listing of the current PPT for 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 nullifying 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)

Current releases of z/OS include an enhancement that changed the behavior of NOPASS. NOPASS now enables a program to bypass RACF dataset protection only when it is executed as a Started Task. New PPT authority NOPASS_ALLOWBATCH can be assigned to a program to enable it to bypass protection when executed as a batch job as well as a Started Task. If a program is assigned NOPASS_ALLOWBATCH, the DSMON SYSPPT report will show ‘BATCH’ under the ‘BYPASS PASSWORD PROTECTION’ column. IBM 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)

SYSTEM-AUDITOR AND ROAUDIT AUTHORITY: Prior to z/OS 2.2, IDs assigned to Auditors, Consultants, and Technical Support staff who needed the ability to examine RACF controls had to be given system-wide AUDITOR authority. Unfortunately, AUDITOR authority also enabled them to change RACF settings related to access monitoring. Based on an enhancement request submitted by RSH Consulting, ROAUDIT authority (Read-Only AUDITOR) was created to give users the ability to examine RACF controls but not make any changes whatsoever. Now, only those users who are responsible for managing security monitoring options should be assigned system-wide AUDITOR authority. Anyone who merely needs to examine RACF controls should instead be given ROAUDIT. (Reference: z/OS Security Server RACF Security Administrator's Guide)

Contact RSH Consulting for training or assistance with auditing RACF.