zed TALKS

2018 ESM Restricted Word / IKJTSO LOGON Survey Responses

Presented by

Richard K. Faulhaber

rkf@newera.com twitter: @faulhaber_rk

Validating New Passwords Against Restricted Word Lists

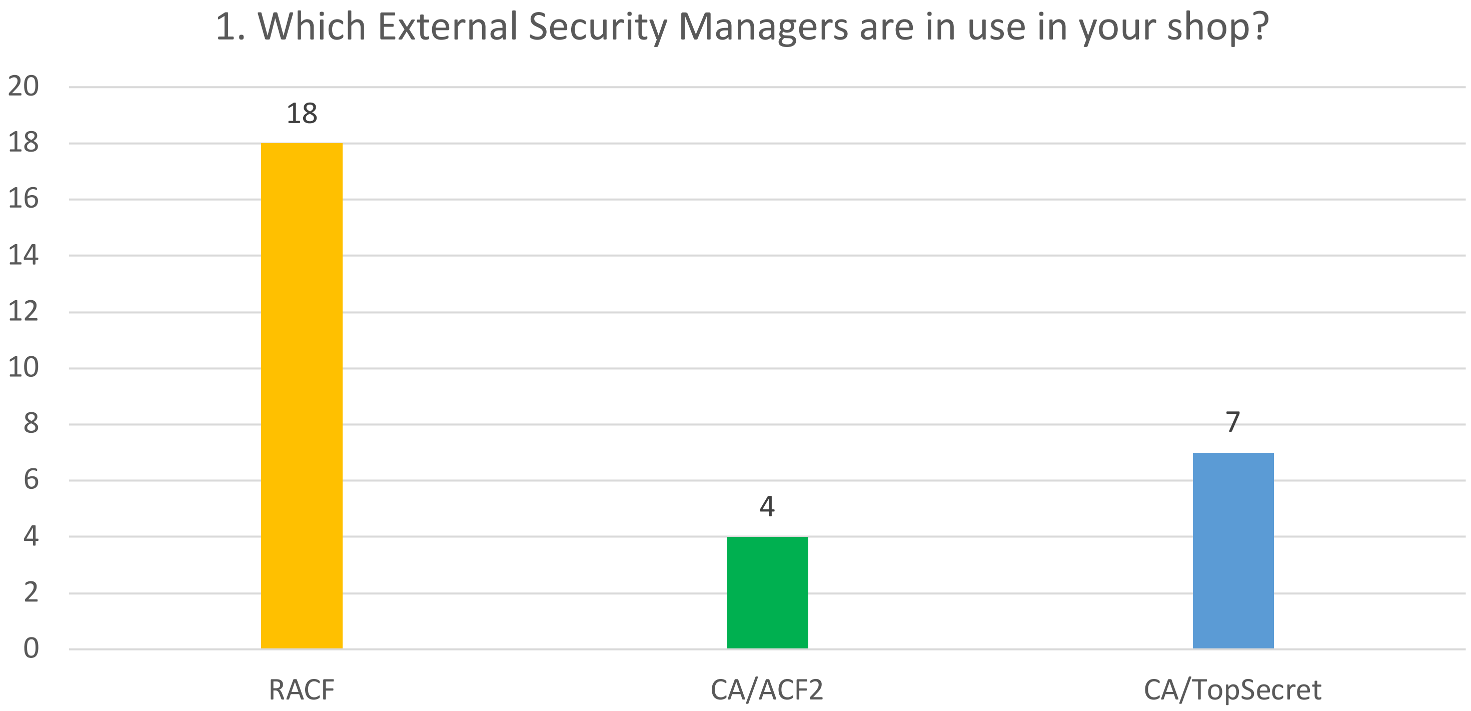
- **New-Password Exit**
- **Native Functionality**
- **Application / Implication**

2018 ESM Restricted Words / IKJTSO LOGON Survey Responses

- RACF does not have a native function for validating new-passwords against a restricted word list.

- CA/ACF2 and CA/Top Secret have native functions to validate new passwords against word lists, however, this functionality is limited.

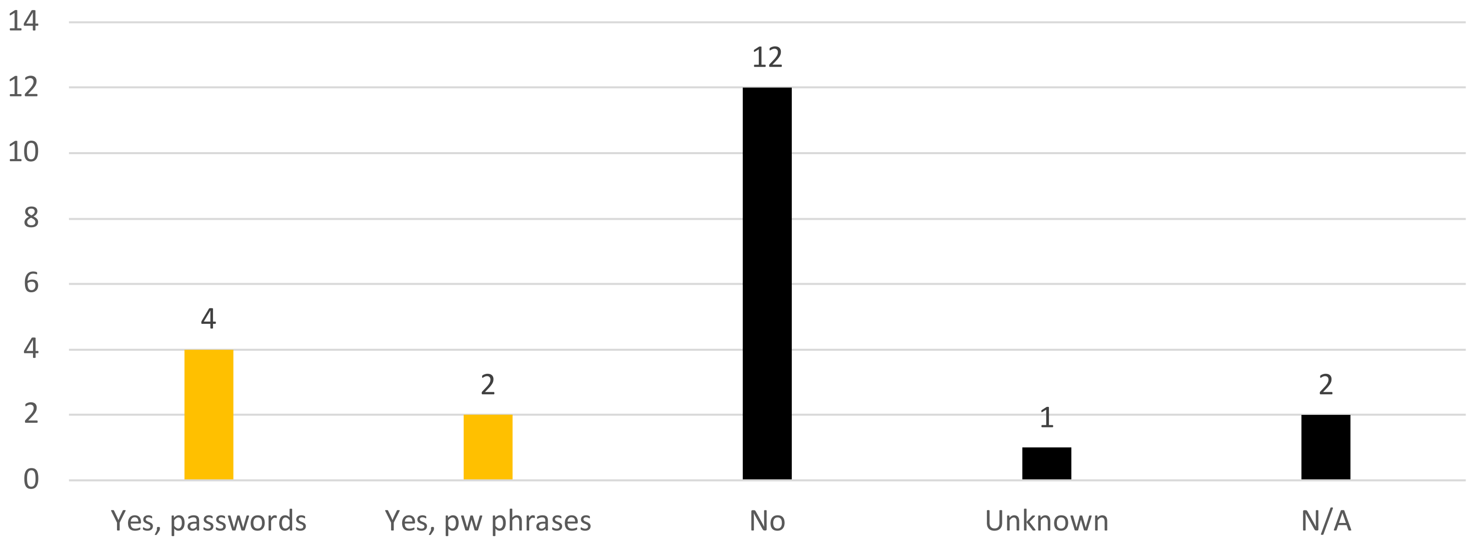
- Through the use of new-password processing exits, all three ESMs are capable of validating against much larger lists.



2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- RACF does not have a native function for validating new-passwords against a restricted word list.

2. For RACF, do you use the new-password and/or the new-password-phrase exit(s) to check new password or new password phrase content against a restricted word list?



- The **US Department of Defense** recommendations for passwords suggest passwords are not to include the user's name, telephone number, userid, or ***any standard dictionary word***. (DOD also recommends not allowing repeated or consecutive characters – RACF can do this with the exit.)

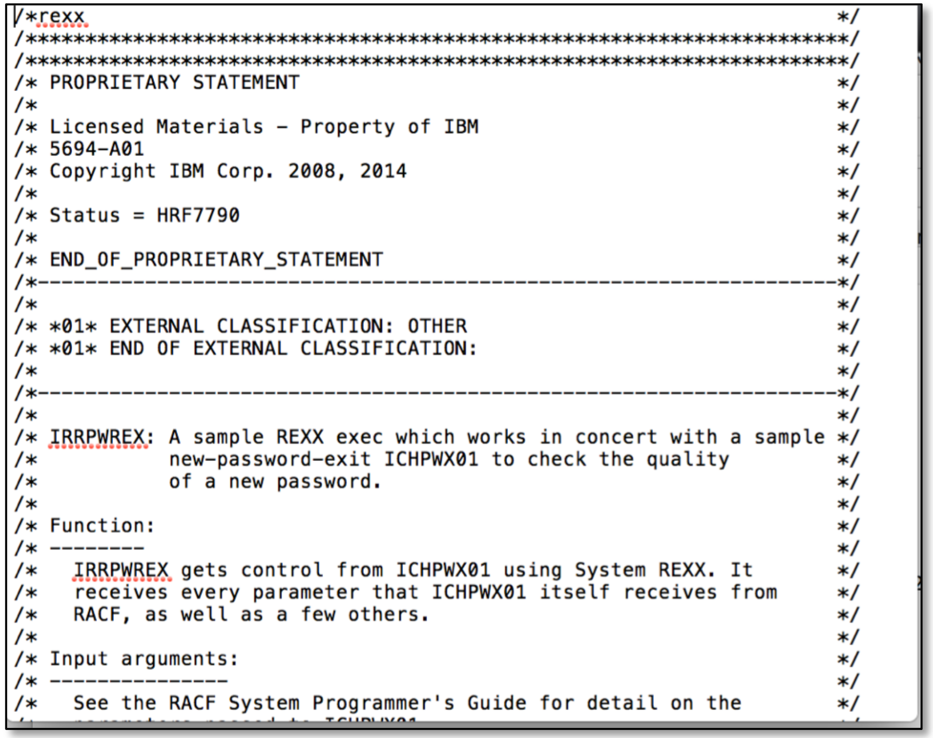
2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

New-password Exit: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.icha200/npeich.htm

ICHPWX01 processing: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.icha200/icha200331.htm

Using the exit for password quality control: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.3.0/com.ibm.zos.v2r3.icha200/neal1.htm

REXX Password Exit sample from IBM:
https://www-03.ibm.com/systems/z/os/zos/features/racf/downloads/rexxpwexit.html



```
/*rexx                                                               */
/*********************************************************************/
/*********************************************************************/
/* PROPRIETARY STATEMENT                                             */
/*                                                                   */
/* Licensed Materials - Property of IBM                              */
/* 5694-A01                                                          */
/* Copyright IBM Corp. 2008, 2014                                    */
/*                                                                   */
/* Status = HRF7790                                                  */
/*                                                                   */
/* END_OF_PROPRIETARY_STATEMENT                                      */
/*-------------------------------------------------------------------*/
/*                                                                   */
/* *01* EXTERNAL CLASSIFICATION: OTHER                               */
/* *01* END OF EXTERNAL CLASSIFICATION:                              */
/*                                                                   */
/*-------------------------------------------------------------------*/
/*                                                                   */
/* IRRPWREX: A sample REXX exec which works in concert with a sample */
/*           new-password-exit ICHPWX01 to check the quality         */
/*           of a new password.                                      */
/*                                                                   */
/* Function:                                                         */
/* --------                                                          */
/*   IRRPWREX gets control from ICHPWX01 using System REXX. It       */
/*   receives every parameter that ICHPWX01 itself receives from     */
/*   RACF, as well as a few others.                                  */
/*                                                                   */
/* Input arguments:                                                  */
/* ---------------                                                   */
/*   See the RACF System Programmer's Guide for detail on the        */
```

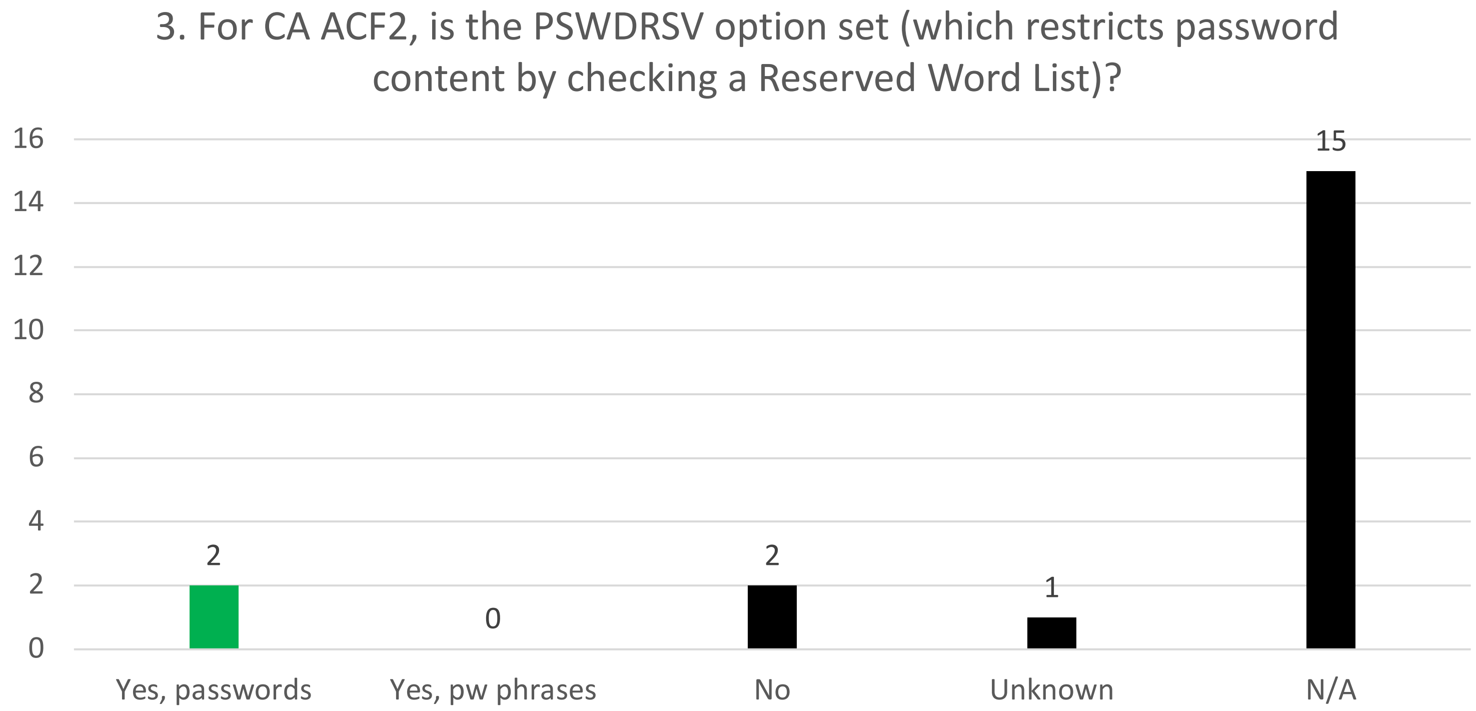
2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

REXX Password Exit sample from IBM can check for:

- Minimum length violation
- Contains disallowed characters
- Does not contain at least one character from a specified number of character types (numbers, letters, special)
- Contains part of user's name
- Is only trivially different from previous value
- Does not contain enough character differences, by position, from previous value
- Contains a word from the restricted dictionary
- Contains too many unchanged characters, by position, from previous value
- Does not contain enough new characters from previous value
- Does not contain all unique characters
- Contains "consecutive" characters
- Contains the user ID, or some subset of the user ID
- Contains too many repeating characters
- Starts with a string from the restricted prefix list
- Uses a restricted pattern

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- The CA/ACF2 Reserved Word List can contain up to 256 entries - one to eight characters long.
- PSWDRSV | NOPSWDRSV specifies whether or not a user can enter a new password that begins with a reserved word prefix.
- PSWDRSV specifies that validation of new passwords does occur.
- NOPSWDRSV specifies that it does not.



- The list of reserved prefixes is specified in the GSO RESWORD infostorage record (known as the Reserved Word Prefix List).

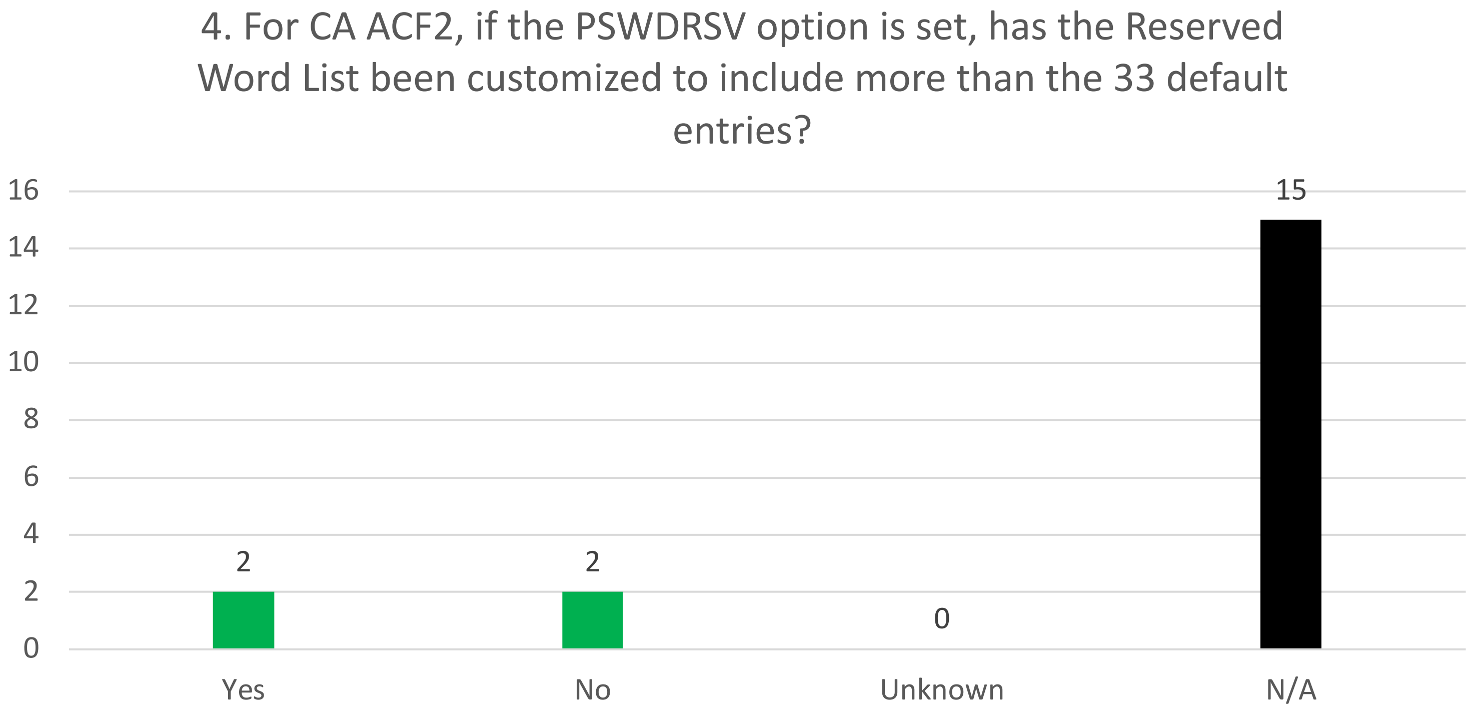
2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

ACF2 – default Reserved Word Prefix List:

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

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- The CA/ACF2 Reserved Word List can contain up to 256 entries - one to eight characters long.

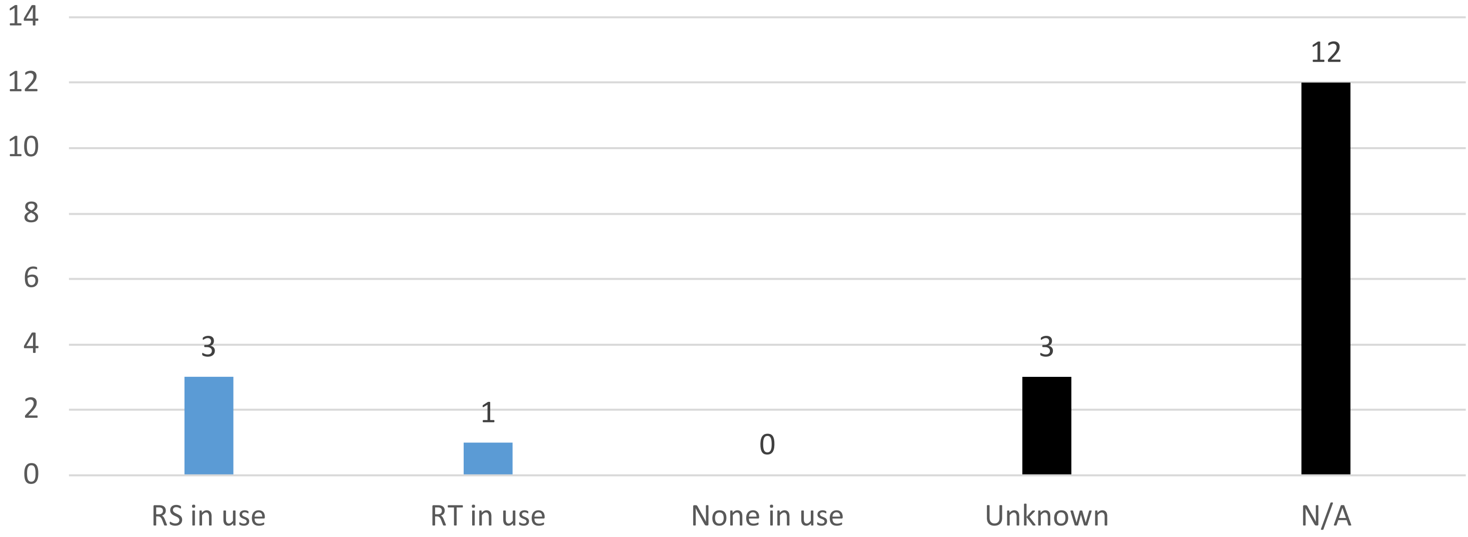


Comment: Use of an in-house utility to screen out words – (ex. Sports team names).

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- NEWPW(RS) and NEWPW(RT), when set, check a user’s new password against the Restricted Password List (RPW).
- The RS option checks to see if the password’s initial characters match one of the password prefix entries in the list.
- The RT option checks to see if the password contains any string that matches an entry from the list.
- CA/Top Secret provides 33 default entries in the list.
- It allows for a maximum of 511 entries.

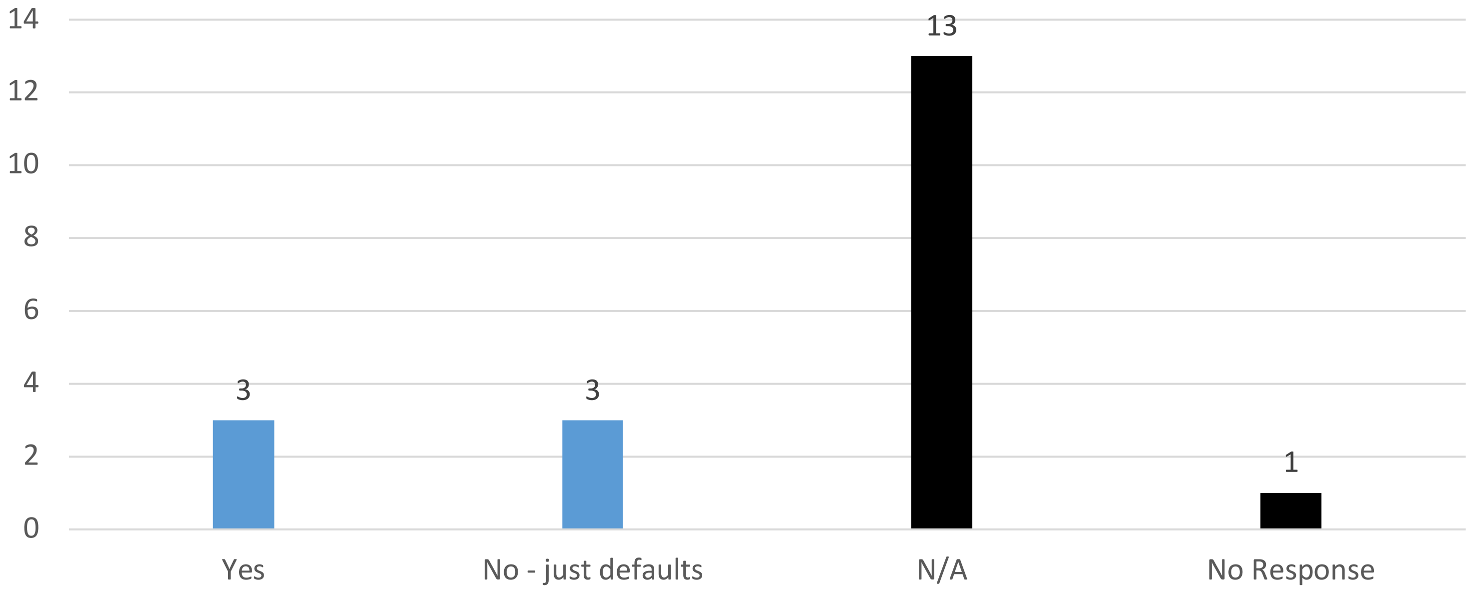
5. For CA Top Secret, are the NEWPW(RS) or NEWPW(RT) options set? These options control whether nor not a new password is checked against the Restricted Password List (RPW).



2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- CA/Top Secret provides 33 default entries in the list.
- It allows for a maximum of 511 entries.

6. For CA Top Secret, if the Restricted Password List (RPW) is in use, has it been customized to include more than the 33 default entries?



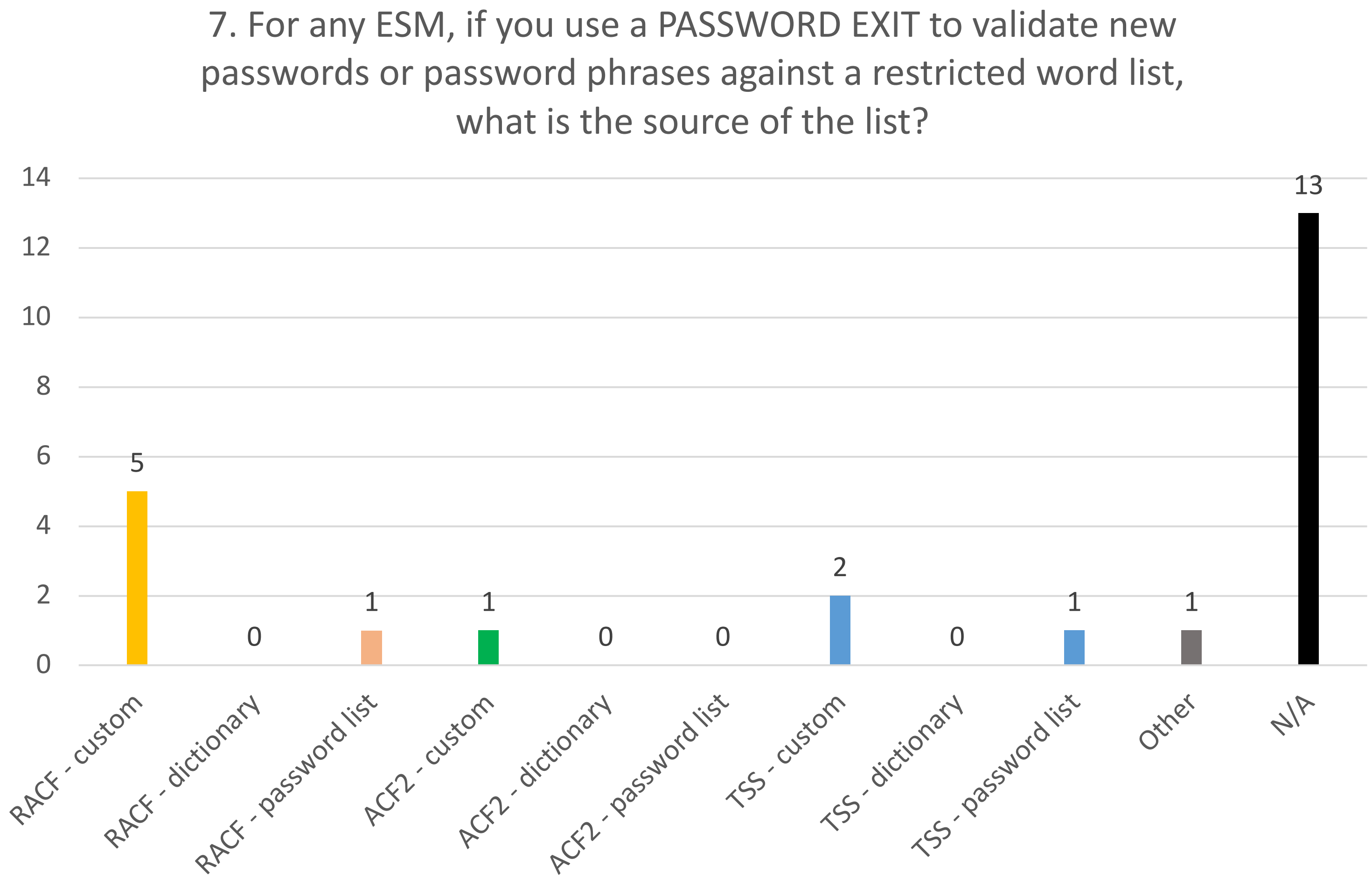
2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

CA/Top Secret – default Restricted Password List:

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

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- Custom / In-House list
- Dictionary word list
- Actual Password list



2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

Comments:

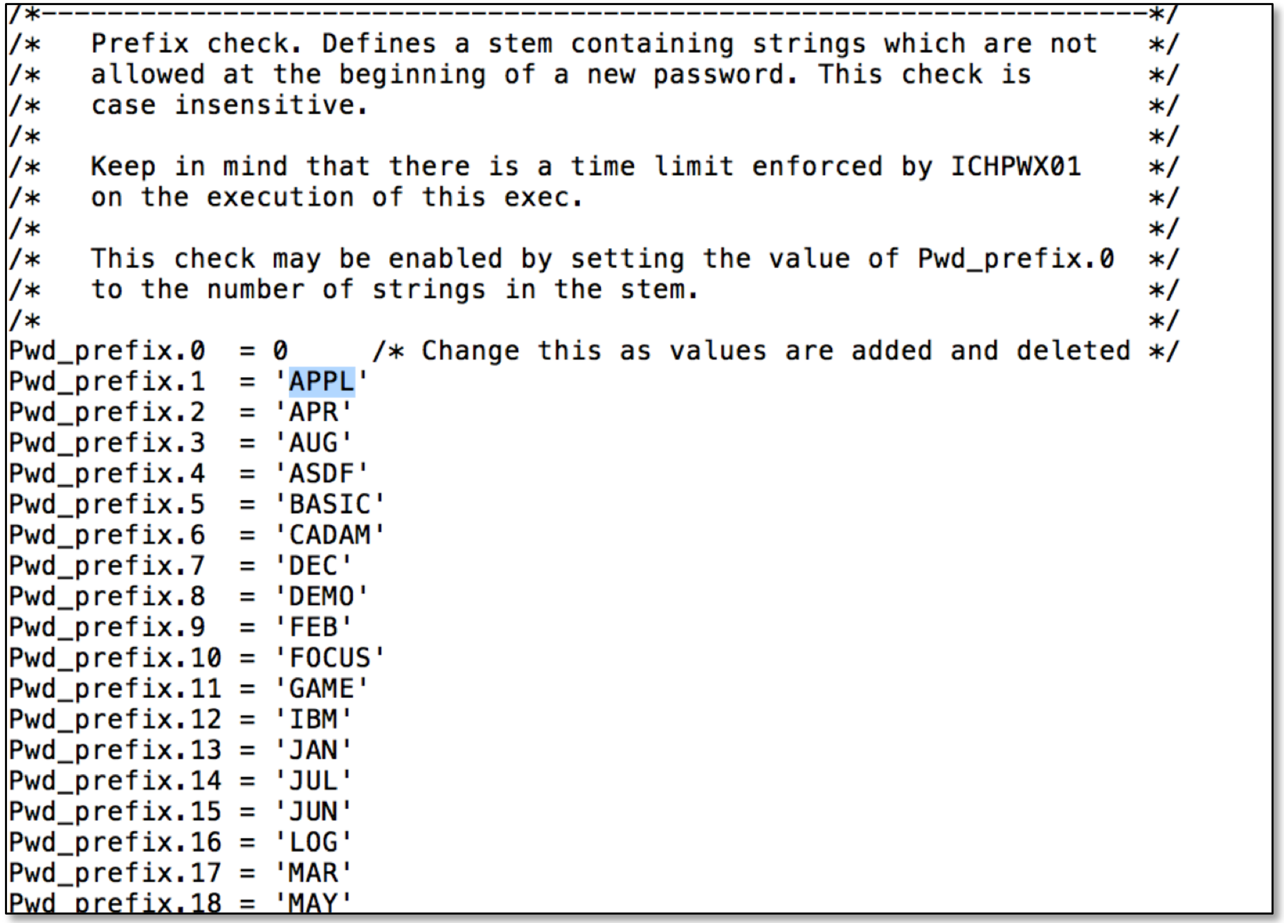
- Customization to prevent:
  - More than 3 characters from prior passwords (within a defined period of time) being used in current password.
  - Use of keyboard sequences (QWERTY or ZAQWSX),
  - Double letters in sequence (like the 2 't's in 'better')
- Minimum character length for passwords
- Requirement for mixture of Alpha, numeric characters.

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

CA/ACF2 Reserved Word List, CA/Top Secret Restricted Password List are identical.

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

RACF sample prefix check code – default contents: identical



```
/*-----------------------------------------------------------------*/
/*   Prefix check. Defines a stem containing strings which are not   */
/*   allowed at the beginning of a new password. This check is       */
/*   case insensitive.                                               */
/*                                                                   */
/*   Keep in mind that there is a time limit enforced by ICHPWX01    */
/*   on the execution of this exec.                                  */
/*                                                                   */
/*   This check may be enabled by setting the value of Pwd_prefix.0  */
/*   to the number of strings in the stem.                           */
/*                                                                   */
Pwd_prefix.0  = 0     /* Change this as values are added and deleted */
Pwd_prefix.1  = 'APPL'
Pwd_prefix.2  = 'APR'
Pwd_prefix.3  = 'AUG'
Pwd_prefix.4  = 'ASDF'
Pwd_prefix.5  = 'BASIC'
Pwd_prefix.6  = 'CADAM'
Pwd_prefix.7  = 'DEC'
Pwd_prefix.8  = 'DEMO'
Pwd_prefix.9  = 'FEB'
Pwd_prefix.10 = 'FOCUS'
Pwd_prefix.11 = 'GAME'
Pwd_prefix.12 = 'IBM'
Pwd_prefix.13 = 'JAN'
Pwd_prefix.14 = 'JUL'
Pwd_prefix.15 = 'JUN'
Pwd_prefix.16 = 'LOG'
Pwd_prefix.17 = 'MAR'
Pwd_prefix.18 = 'MAY'
```

National Institute of Standards and Technology - Recommendation

NIST Special Publication 800-63b https://pages.nist.gov/800-63-3/sp800-63b.html
Appendix A—Strength of Memorized Secrets - A.3 Complexity

“Users’ password choices are very predictable, so attackers are likely to guess passwords that have been successful in the past. These include dictionary words and passwords from previous breaches, such as the “Password1!” example above. For this reason, it is recommended that passwords chosen by users be compared against a “black list” of unacceptable passwords. This list should include passwords from previous breach corpuses, dictionary words, and specific words (such as the name of the service itself) that users are likely to choose. Since user choice of passwords will also be governed by a minimum length requirement, this dictionary need only include entries meeting that requirement.”

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

Most people agree on what makes a BAD password

- Personal information
- Dictionary words
- Commonly known (leaked) passwords
  - Probable word lists * : https://github.com/berzerk0/Probable-Wordlists
  - Worst Passwords * : https://twitter.com/WorstPasswords

* Github for Berzerk0: https://github.com/berzerk0

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

Top 207 Worst Passwords *

* Reference: https://github.com/berzerk0/Probable-Wordlists

123456
password
123456789
12345678
12345
qwerty
123123
111111
abc123
1234567
dragon
1q2w3e4r
sunshine
654321
master
1234
football
1234567890
000000
computer
666666
superman
michael
internet
iloveyou
daniel
1qaz2wsx
monkey
shadow
jessica
letmein
baseball
whatever
princess
abcd1234
123321
starwars
121212
thomas
zxcvbnm
trustno1
killer
welcome
jordan
aaaaaa
123qwe
freedom
password1
charlie
batman
jennifer
7777777
michelle
diamond
oliver
mercedes
benjamin
11111111
snoopy
samantha
victoria
matrix
george
alexander
secret
cookie
asdfgh
987654321
123abc
orange
f****ou
asdf1234
pepper
hunter
silver
joshua
banana
1q2w3e
chelsea
1234qwer
summer
qwertyuiop
phoenix
andrew
q1w2e3r4
elephant
rainbow
mustang
merlin
london
garfield
robert
chocolate
112233
samsung
qazwsx
matthew
buster
jonathan
ginger
flower
555555
test
caroline
amanda
maverick
midnight
martin
junior
88888888
anthony
jasmine
creative
patrick
mickey
123
qwerty123
cocacola
chicken
passw0rd
forever
william
nicole
hello
yellow
nirvana
justin
friends
cheese
tigger
mother
liverpool
blink182
asdfghjkl
andrea
spider
scooter
richard
soccer
rachel
purple
morgan
melissa
jackson
arsenal
222222
qwe123
gabriel
ferrari
jasper
danielle
bandit
angela
scorpion
prince
maggie
austin
veronica
nicholas
monster
dexter
carlos
thunder
success
hannah
ashley
131313
stella
brandon
pokemon
joseph
asdfasdf
999999
metallica
december
chester
taylor
sophie
samuel
rabbit
crystal
barney
xxxxxx
steven
ranger
patricia
christian
a***ole
spiderman
sandra
hockey
angels
security
parker
heather
888888
victor
harley
333333
system
slipknot
november
jordan23
canada
tennis
qwertyui
casper

IKJTSO LOGON Options

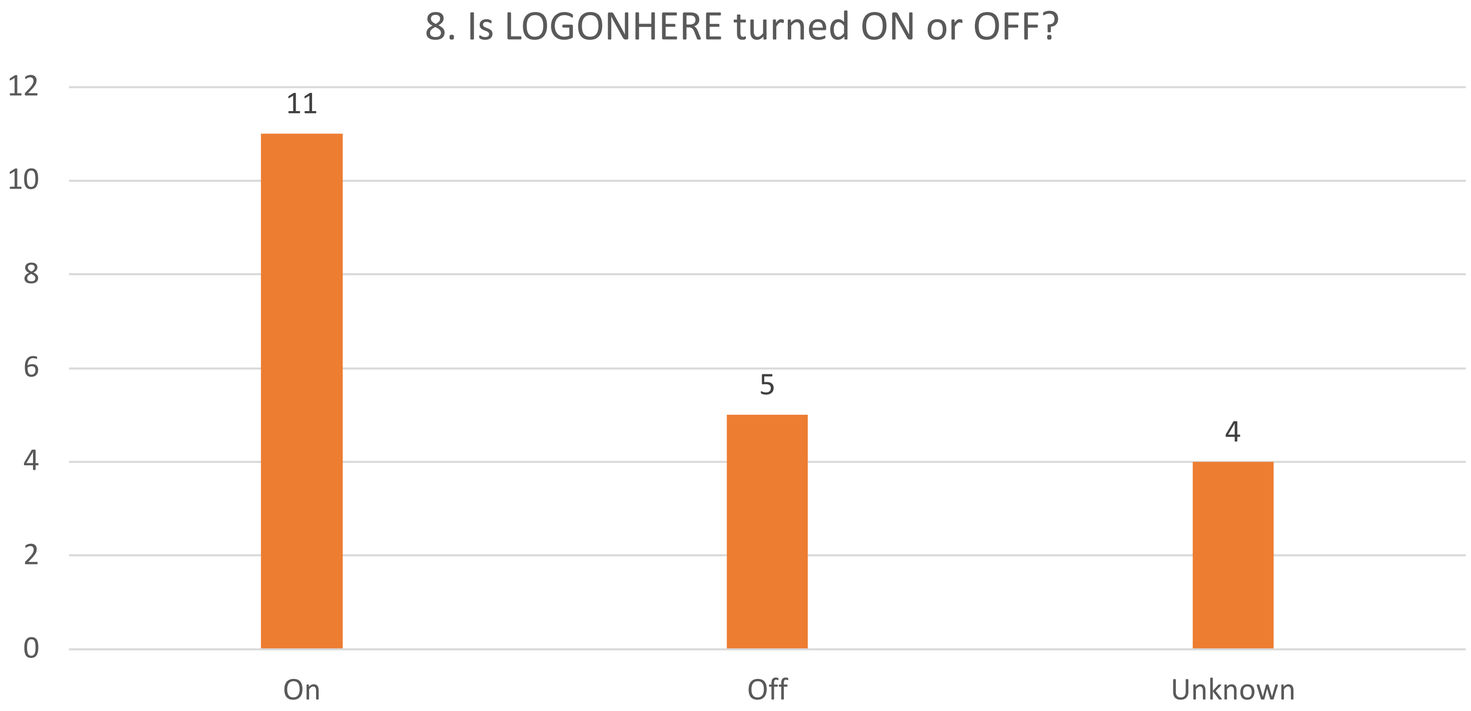
- **LOGONHERE**
- **PASSPHRASE**
- **PASSWORDPREPROMPT (*new in V2R2*)**
- **USERIDMAX (*new in V2R3*)**
- **VERIFYAPPL**

IBM Documentation: z/OS MVS Init and Tuning Reference – IKJTSOxx (TSO/E commands & programs
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.ieae200/ikjtso.htm

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

This parameter specifies whether the RECONNECT option on the TSO/E LOGON panel is honored even when the system does not detect a disconnected state and the user appears to be logged on.

Default value: ON

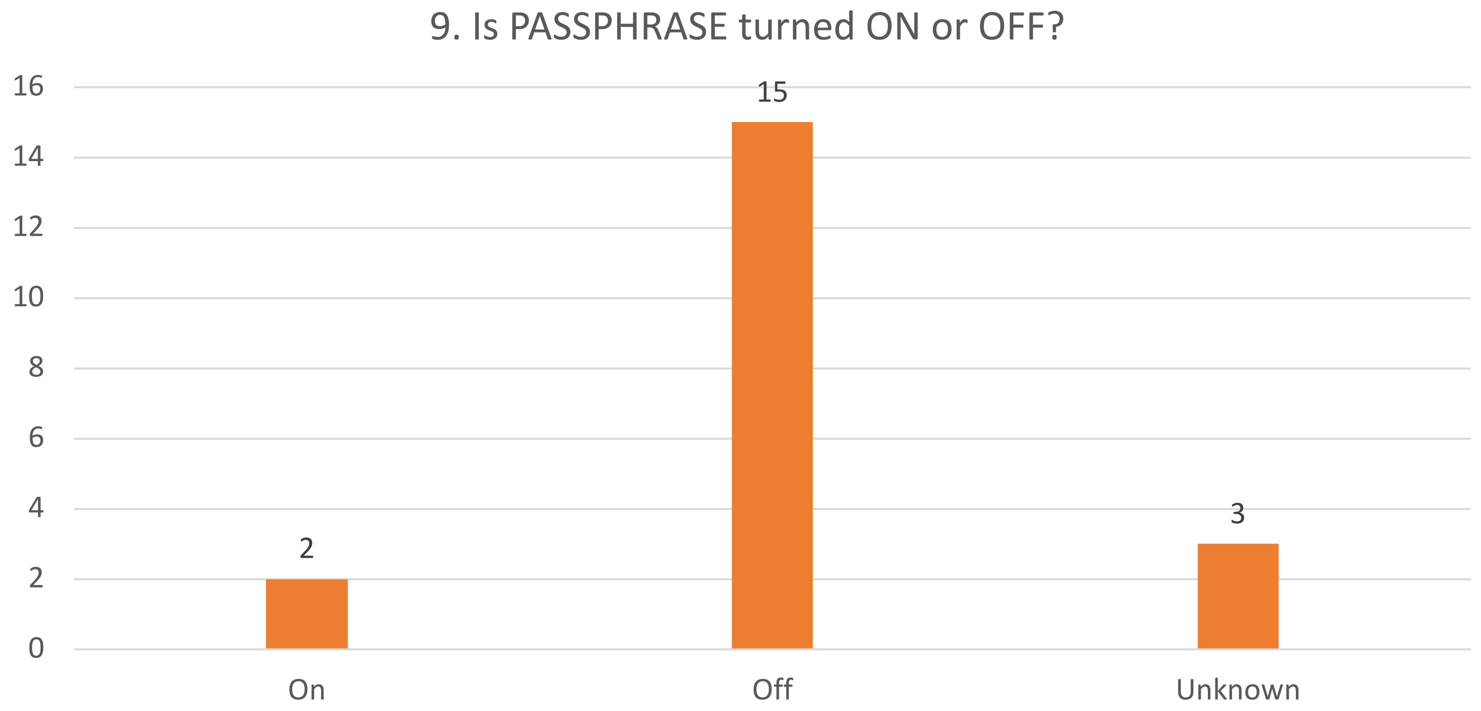


When set to ON, this parameter allows a user ID to be logged on to more than one TSO session.

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

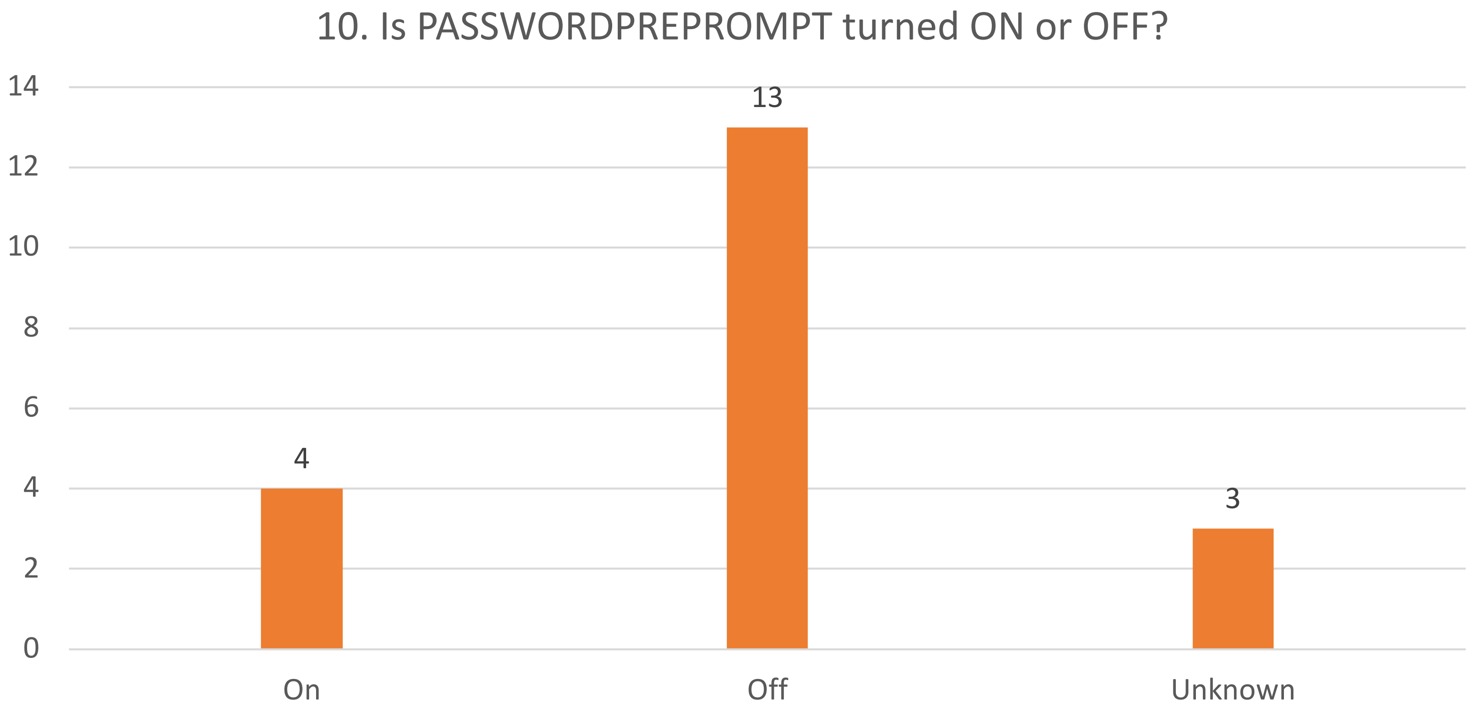
This parameter specifies whether the TSO/E LOGON panel allows users to enter up to 100 characters in the password field.

Default value: OFF



2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- This parameter specifies whether the user will be prompted to enter both the user ID and password prior to the presentation of any other information.
- Default value: OFF
- New in V2R2



NOTES: This is to prevent the disclosure if information about a failed logon attempt as to whether that failure was due to the Userid, the Password, or both.

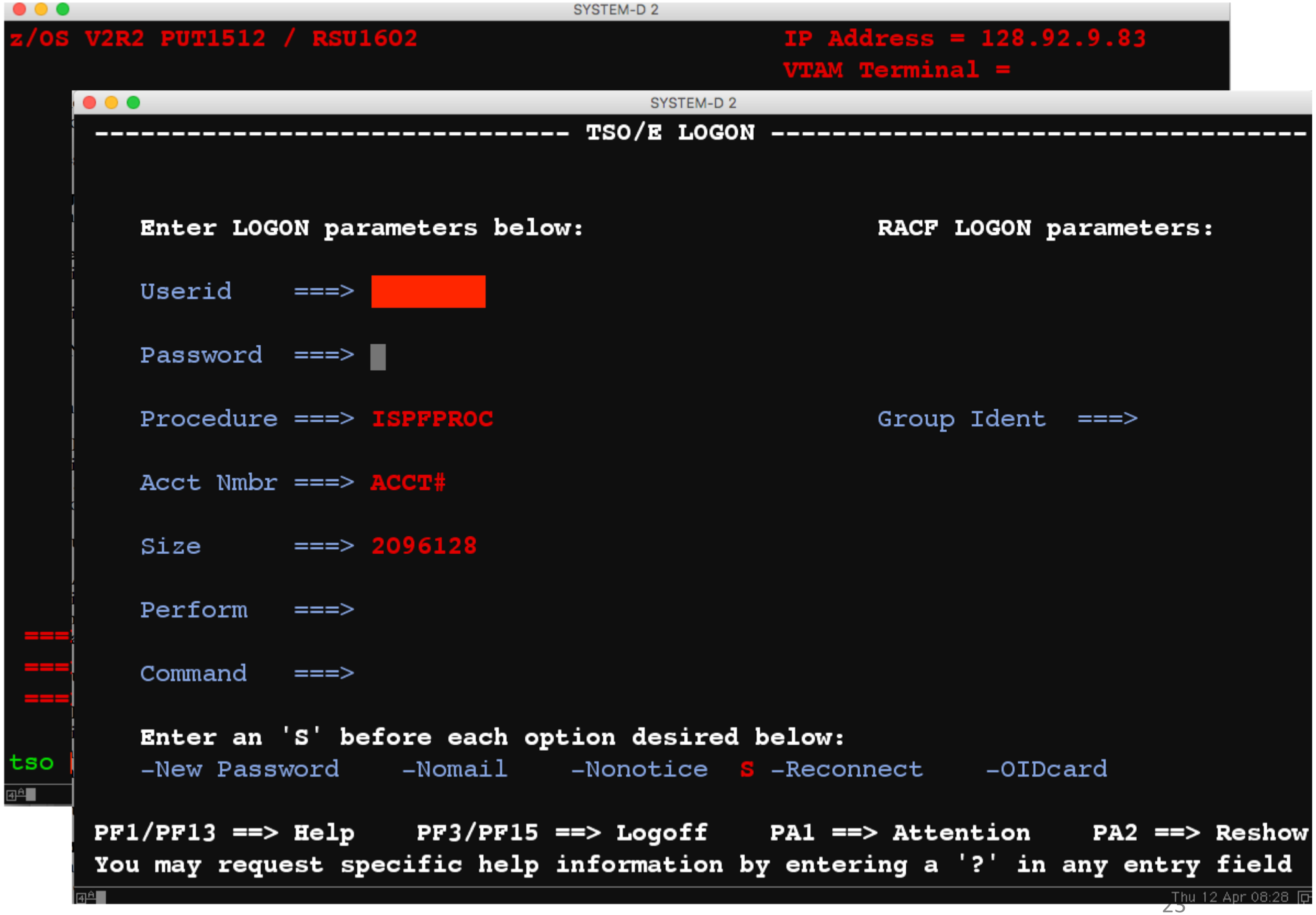
Telling the user that the password is incorrect, tells that user that the UserID is valid.

A hacker can use this information to enumerate userIDs on a system (see Phil Young's SHARE presentation.)

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- When PASSWORDPREPROMPT is OFF, the TSO/E LOGON screen appears, which contains logon information.

- Default value: OFF

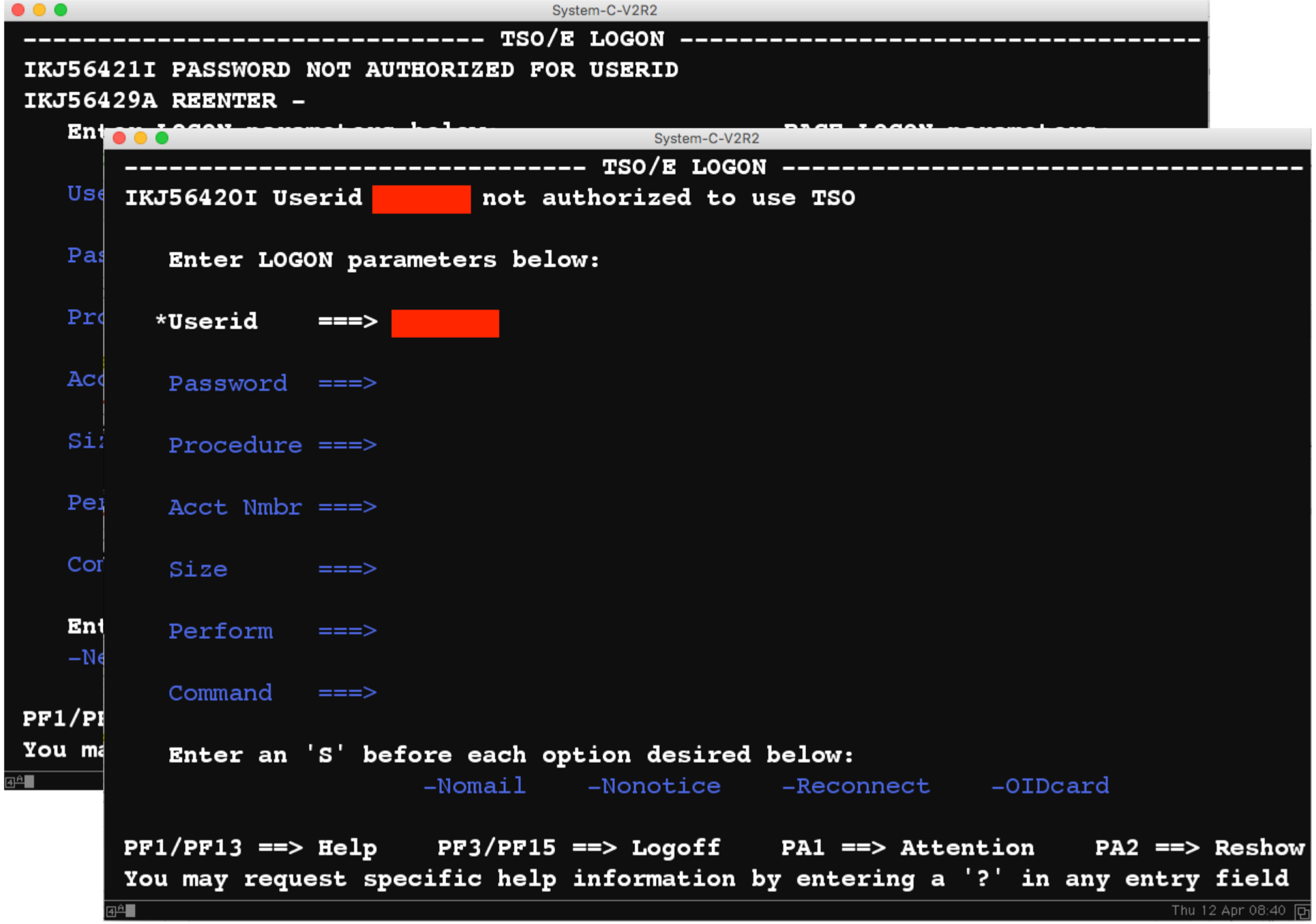


```
z/OS V2R2 PUT1512 / RSU1602                              IP Address = 128.92.9.83
                                                         VTAM Terminal =
===
===
===
tso
```

```
------------------------------- TSO/E LOGON -----------------------------------


   Enter LOGON parameters below:                        RACF LOGON parameters:

   Userid    ===> [redacted]

   Password  ===>

   Procedure ===> ISPFPROC                              Group Ident  ===>

   Acct Nmbr ===> ACCT#

   Size      ===> 2096128

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
   -New Password    -Nomail    -Nonotice   S -Reconnect    -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- When PASSWORDPREPROMPT is OFF, the TSO/E LOGON screen appears, which contains logon information.
- If either the UserID or the Password is invalid or incorrect, the TSO/E LOGON panel will tell you that.
- Default value: OFF



System-C-V2R2

```
------------------------------- TSO/E LOGON -----------------------------------
IKJ56421I PASSWORD NOT AUTHORIZED FOR USERID
IKJ56429A REENTER -
   Ent
   Use
   Pas
   Pro
   Acc
   Siz
   Per
   Con
   Ent
   -Ne
PF1/PF
You ma
```

System-C-V2R2

```
------------------------------- TSO/E LOGON -----------------------------------
IKJ56420I Userid [redacted] not authorized to use TSO

   Enter LOGON parameters below:

  *Userid    ===> [redacted]

   Password  ===>

   Procedure ===>

   Acct Nmbr ===>

   Size      ===>

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
                  -Nomail     -Nonotice     -Reconnect     -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

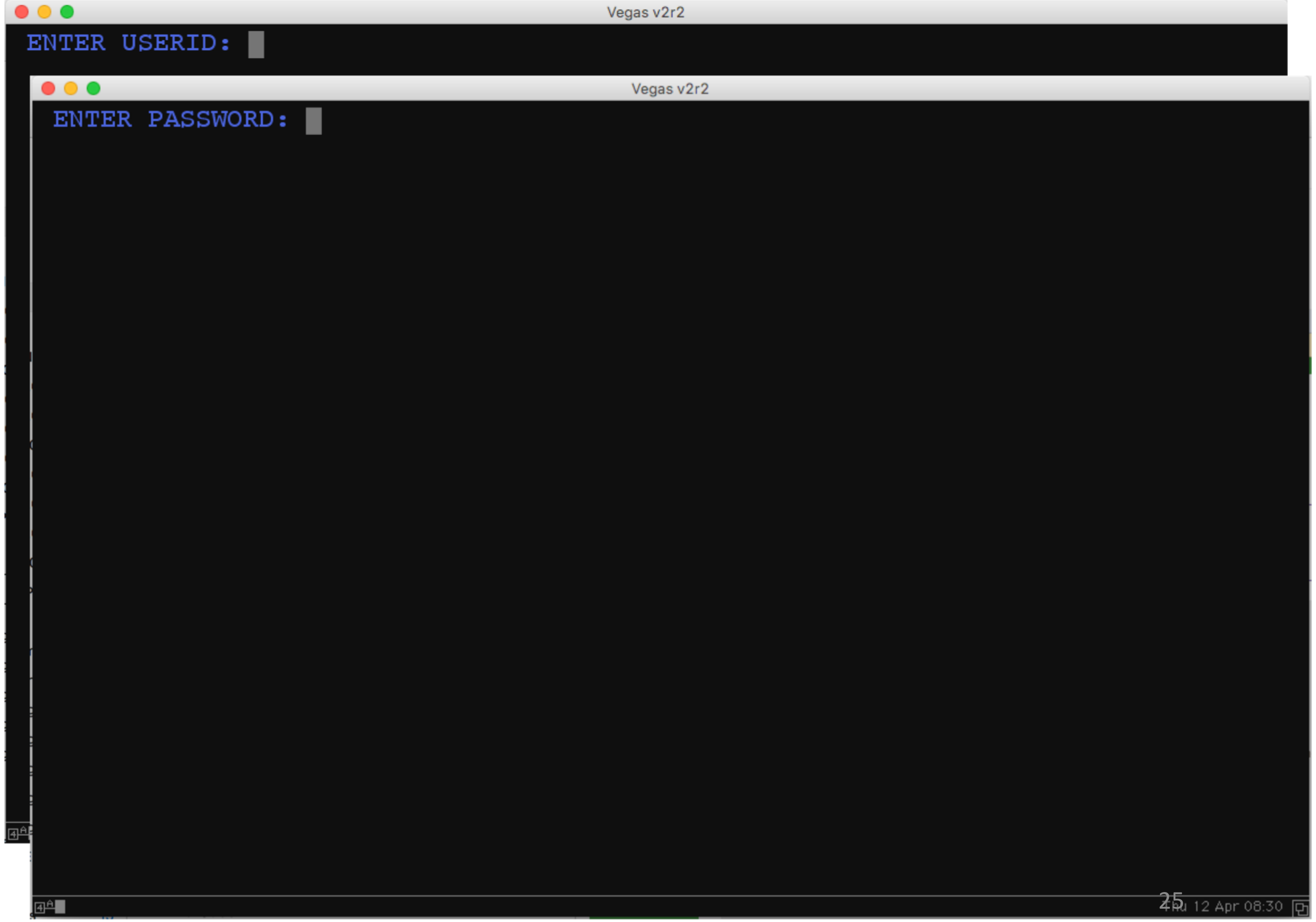
Thu 12 Apr 08:40

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- When PASSWORDPREPROMPT is ON, the TSO/E LOGON screen is not displayed until both the UserID and Password have been entered in separate screens.

- If either one is invalid, the TSO/E LOGON screen is not displayed and no message is given to indicate which (UserID or Password) was incorrect or invalid.

- Default value: OFF

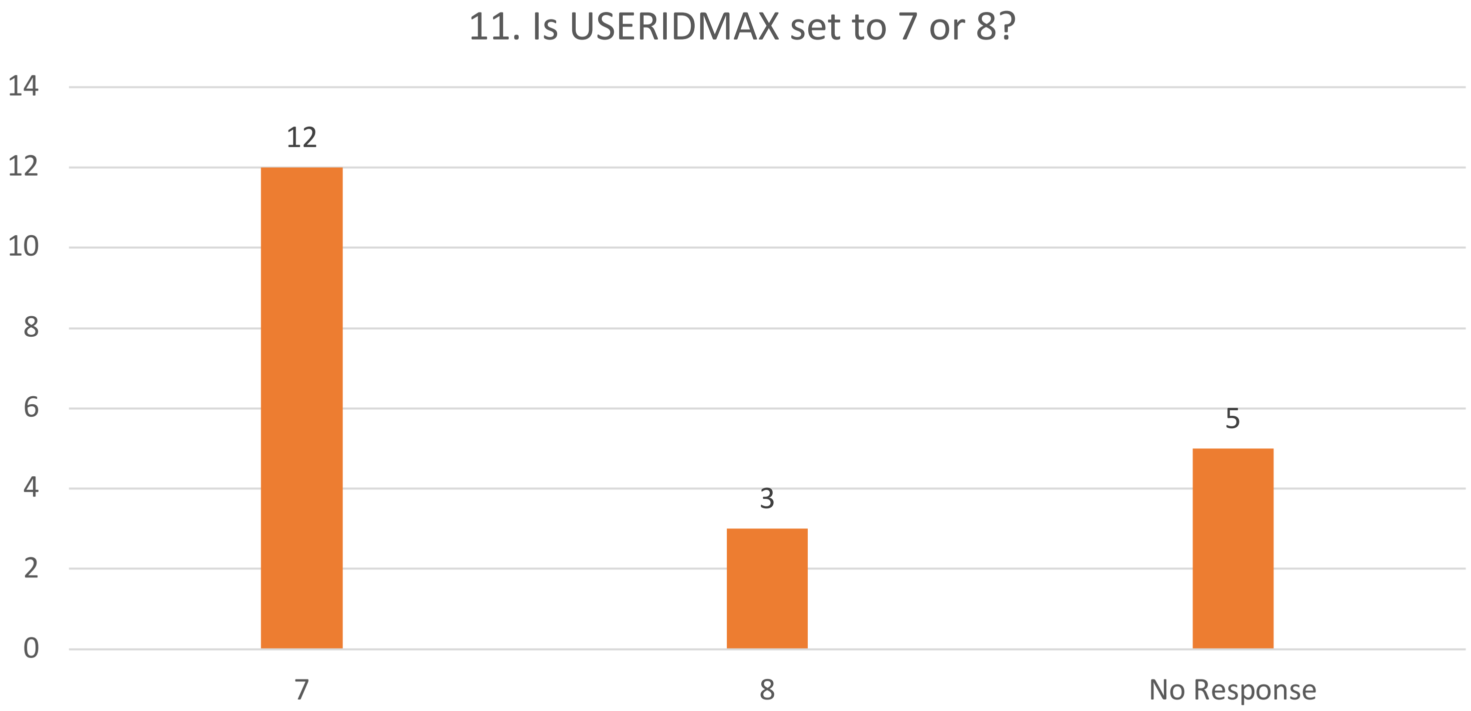


```
ENTER USERID:
```

```
ENTER PASSWORD:
```

2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- This parameter allows setting a longer user ID or prefix.
- Default value: 7
- New in V2R3

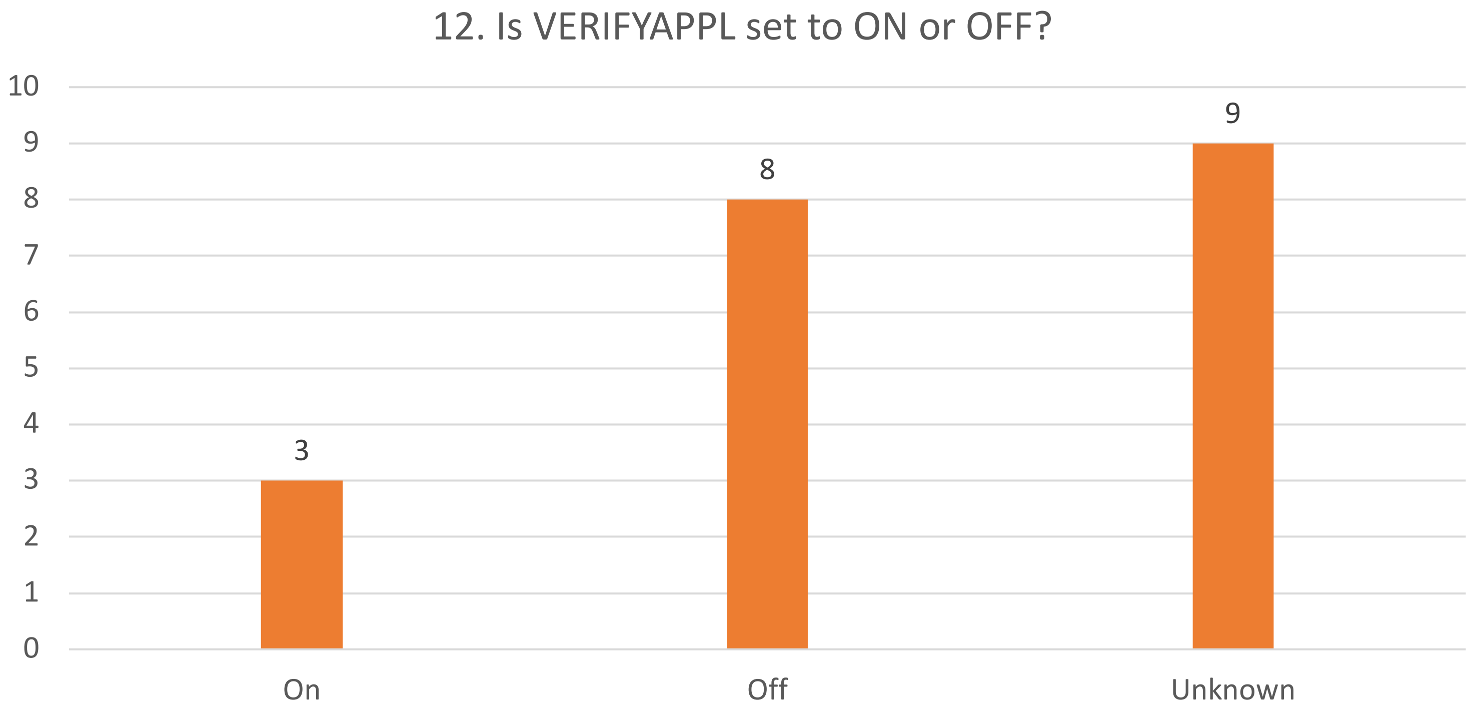


2018 ESM Restricted Words – IKJTSO LOGON Survey Responses

- This parameter specifies whether TSO/E determines an APPLID for the system the user is logging on to and passes that APPLID to RACF for verification during TSO/E logon.

- This option can be used to limit access to different systems that share a RACF database.

- Default value: OFF



Q&A

Richard K. Faulhaber
rkf@newera.com twitter: @faulhaber_rk

THE z EXCHANGE
Reaching Out to the z Community Worldwide

zed TALKS

NEWERA