Payment Card Industry (PCI)

Challenges and Issues for RACF Systems

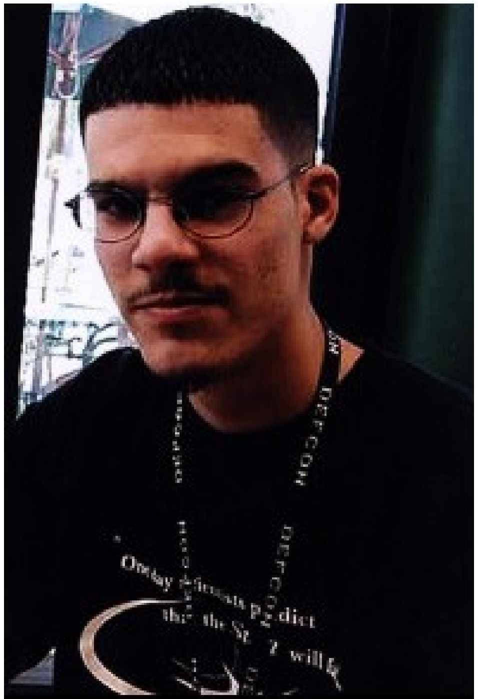
Jim Yurek
Vanguard Integrity Professionals

February 28, 2011
Session Number 8507

The Problem: Credit Card Breaches

As long as we have the Internet and a “Black Market” for Credit Cards, We’ll continue to have Breaches

Albert Gonzalez, dubbed his operation: “Operation Get Rich or Die Tryin’”



Albert Gonzalez at the 2001 DefCon hackers' convention in Las Vegas

Captured

Convicted for breaches at:

- ✓ TJX Corp (45M)
- ✓ Heartland Payment Systems (100M)
- ✓ Hannaford Bros Co (4.2M)
- ✓ 7-Eleven (TBD)
- ✓ 2 Unidentified Companies (TBD)

Albert also infiltrated these companies for over 40 million credit cards:

- ✓ BJ's Wholesale Club
- ✓ Barnes & Noble Inc
- ✓ Office Max
- ✓ Dave & Buster's
- ✓ DSW shoe stores
- ✓ Forever 21

Forester Report, April 15, 2008

PCI Compliance and the Costs of a Credit Card Breach

TJX is the poster child for credit card breaches

- Hackers spent 18 months exploiting weak wireless security outside thousands of TJX stores
- Estimated download, 100 million credit cards and other personal information
- TJX estimated the breach will cost 116 million dollars
- Others estimate the cost at 1.2 billion dollars

Forester went on to say that:

- Breaches are occurring more often than people realize
- Only 31 states have laws requiring credit card breach disclosures
- If a company is breached, the business and PR risks are tremendous
- The average cost per breached card will be between $90 and $305

The PCI Data Security Standards

Six Categories and 12 Major Requirements

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security

The PCI Data Security Standards

Requirements have Requirements

8.5 Ensure proper user authentication

- 8.5.1 Control the addition, deletion and modification of user IDs
- 8.5.2 Verify user identity before performing password resets
- 8.5.3 Set first-time passwords to a unique value
- 8.5.4 Immediately revoke access for any terminated users
- 8.5.5 Remove/disable inactive user accounts at least every 90 days
- 8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed
- 8.5.7 Communicate password procedures and policies to all users who have access to cardholder data
- 8.5.8 Do not use group, shared or generic accounts and passwords
- 8.5.9 Change user passwords at least every 90 days
- 8.5.10 Require a minimum password length of at least seven characters
- 8.5.11 Use passwords containing both numeric and alphabetic characters
- 8.5.12 Don’t allow a new password that is the same as any of the last four passwords used
- 8.5.13 Limit repeated password attempts by locking out the ID after not more than six attempts
- 8.5.14 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID

The Challenge: Knowing what to Review

What's more important, the "Requirement" or "Testing Procedure"?

PCI DSS Requirement	Testing Procedure
8.5.9 Change user passwords at least every 90 days.	8.5.9.a For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.
8.5.10 Require a minimum password length of at least seven characters.	8.5.10.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	8.5.12.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	8.5.13.a For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.

The Challenge: Identifying “System Components”

You must interpret the meaning of “System Components” for mainframes

PCI DSS applies to all in-scope “System Components”

- ✓ 17 Requirements contain the phrase “System Components”
- ✓ 38 Testing Procedures contain the phrase “System Components”

System components are defined as:

- ✓ Network components
  - include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and security appliances.
- ✓ Server types
  - include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).
- ✓ Applications
  - include all purchased and custom applications, including internal and external (Internet) applications.

The Challenge: Identifying “System Components”

Different Interpretations of a z/OS “System Component”

1st Systems Programmer	2nd Systems Programmer	RACF Engineer	RACF Administrator
✓ Master Catalog	✓ SDSF	✓ The RACF Database	✓ Dataset Profiles
✓ APF Authorized Datasets	✓ Session Managers	✓ Copies of the RACF database	✓ General Resource Profiles
✓ LINKLIB Datasets	✓ SYS1.UADS Dataset	✓ SETROPTS Settings	✓ User ID Attributes
✓ User Catalogs	✓ WebSphere	✓ RACF CDT	✓ Group Connect Authorities
✓ RACF Database	✓ JES2 / JES3	✓ RACF Classes	✓ Role Based Access
✓ Parmlib Datasets	✓ OMEGAMON	✓ General Resource Profiles	**DBA**
✓ Multi-User Access Systems	✓ WebSphere MQ	✓ SMF log files	✓ IMS Databases
✓ z/OS Security Patches	✓ DFSMS	✓ Group Membership	✓ DB2 Databases
✓ System Proclibs	✓ SVC’s	✓ Privileged Userids	✓ DB2 Table Trace
✓ Started Tasks	✓ CICS System Datasets	✓ RACF Exits	✓ Oracle Databases
✓ SYS1.Parmlib	✓ DB2 System Datasets	✓ RACF Tables	✓ RACF Classes for DB2
✓ SMF Log Files	✓ IBM Communications Server	✓ IRR Prefixed Utilities	✓ IDMS
✓ System Exits	✓ Vendor Security Products	✓ Logging Parameters	**QSA or Compliance Mgr.**
✓ DASD Volume Backups	✓ DASD Volume Backups	✓ Role Based Access	?

The Challenge: Knowing What to Review

Assignment of Privileges

PCI DSS Requirement	Testing Procedure
7.2.2 Assignment of privileges to individuals based on job classification and function	7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.

Things to consider:

- ✓ system-Special, Operations and Auditor attributes
- ✓ group-Special, Operations and Auditor attributes
- ✓ CLAUTH Authority
- ✓ Connect Authority (Join, Connect, Create)
- ✓ Connect Groups vs. Functional Groups
- ✓ RBA Groups on access lists vs. Userids

The Challenge: Knowing What to Review

Default “Deny-all Setting

PCI DSS Requirement	Testing Procedure
7.2.3 Default “deny-all” setting	7.2.3 Confirm that the access control systems have a default “deny-all” setting

Does RACF have a “deny-all” setting?

- ✓ PROTECTALL

Also consider the following:

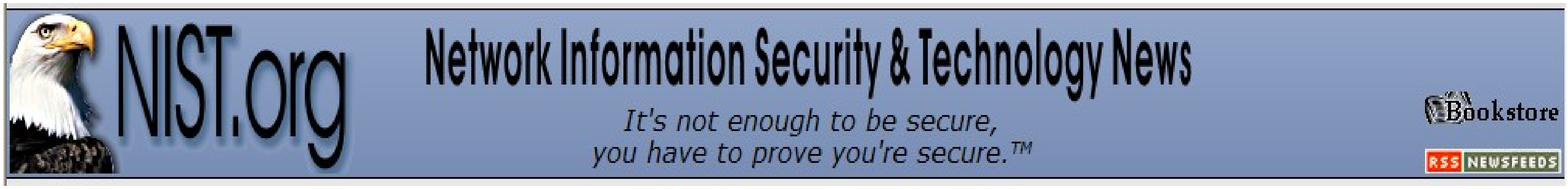
- ✓ Universal Access greater than READ
- ✓ ID(*)
- ✓ WARNING
- ✓ Global Access Table
- ✓ Inactive RACF Classes
- ✓ The Dataset Name Conversion Table
- ✓ RACF Exits

The Challenge: Proving Compliance

Providing Acceptable “Supporting Documentation”

NIST trademarked the phrase:

“It’s not enough to be secure, you have to prove you’re secure. TM “



It's not enough to be secure,
you have to prove you're secure.™

- ✓ **It’s impossible to be complaint without DOCUMENTATION, and Lots of it !!!**
- ✓ **Even if you are compliant, if Records Don’t Exist to Prove It, It May Not Count**
- ✓ **Going forward, there will be increased pressure on merchants and service providers to provide adequate “supporting documentation” to support annual assessments**

The Challenge: Proving Compliance

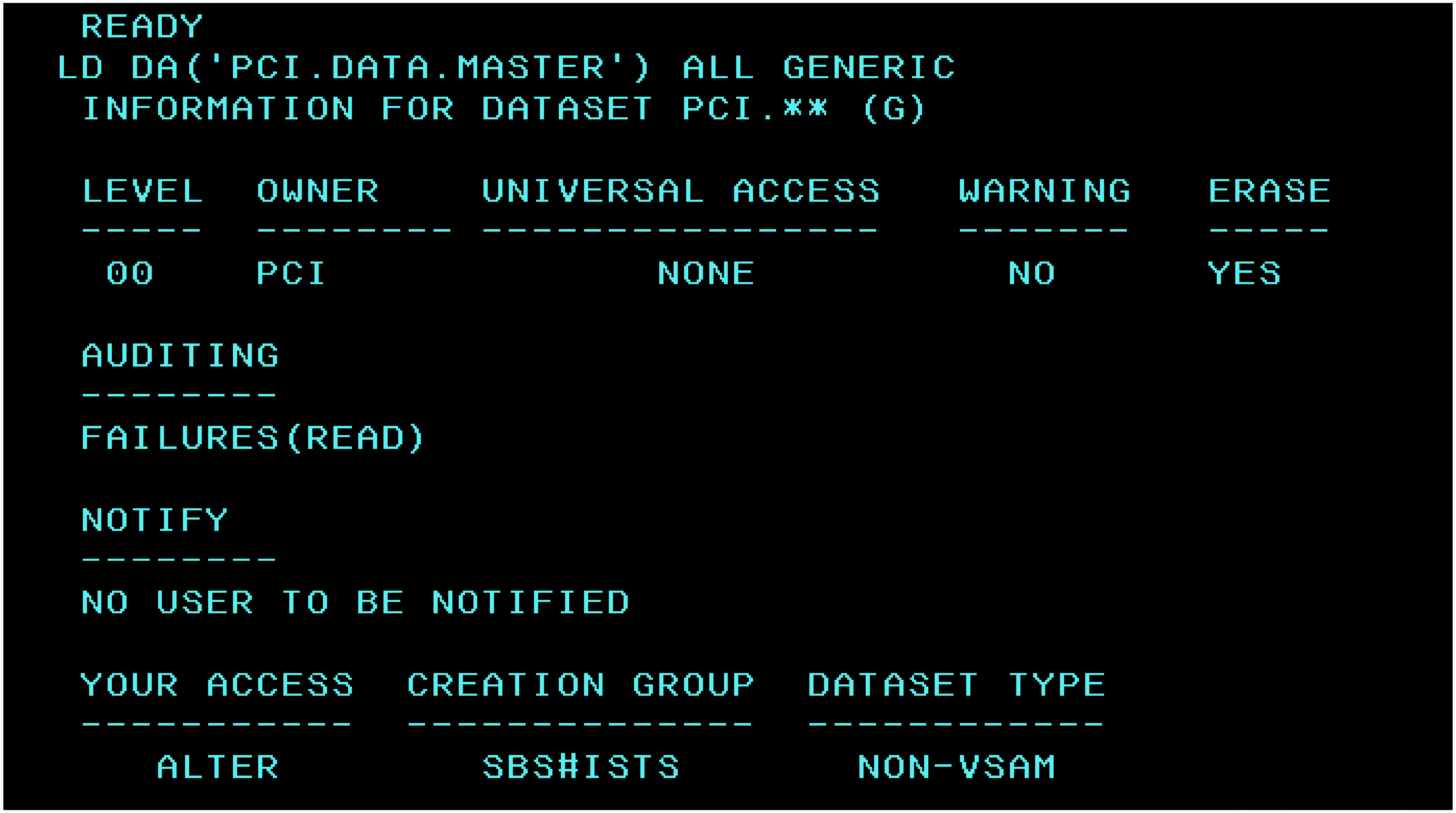
Is an “Online Display” Acceptable Supporting Documentation ?

```
 READY
LD DA(‘PCI.DATA.MASTER') ALL GENERIC

 INFORMATION FOR DATASET PCI.** (G)

 LEVEL  OWNER  UNIVERSAL  ACCESS   WARNING   ERASE
 ----------  ---------   -------------------------------  --------------  ----------
  00        PCI                  NONE                      NO              YES

 AUDITING
 -------------------------
 FAILURES(READ)

 NOTIFY
 --------
 NO USER TO BE NOTIFIED
```

SHARE in Anaheim 2011

The Challenge: Proving Compliance

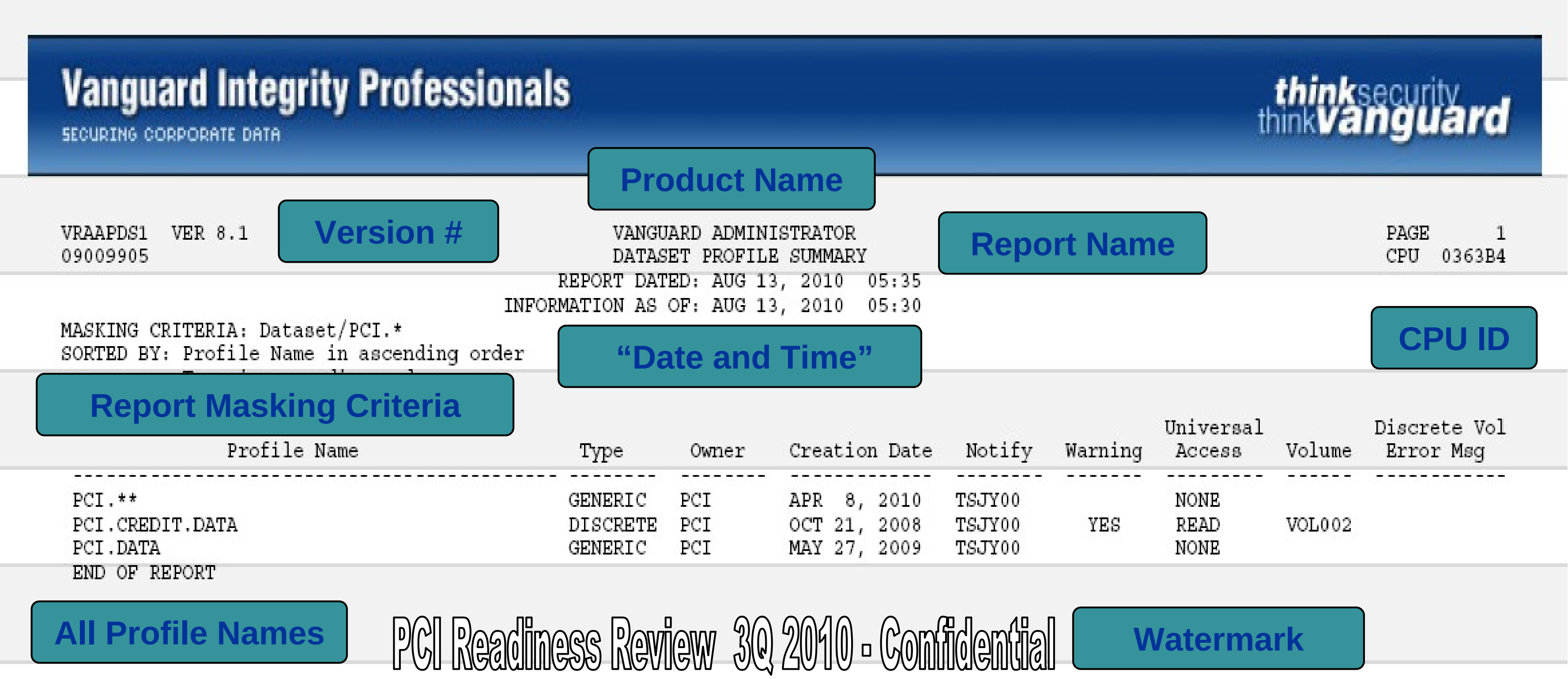
Is a “Screen-Shot” Acceptable Supporting Documentation ?



```
 READY
LD DA('PCI.DATA.MASTER') ALL GENERIC
 INFORMATION FOR DATASET PCI.**  (G)

 LEVEL  OWNER    UNIVERSAL ACCESS   WARNING   ERASE
 -----  -------- ----------------   -------   -----
  00    PCI             NONE          NO      YES

 AUDITING
 --------
 FAILURES(READ)

 NOTIFY
 --------
 NO USER TO BE NOTIFIED

 YOUR ACCESS  CREATION GROUP  DATASET TYPE
 -----------  --------------  ------------
    ALTER        SBS#ISTS       NON-VSAM
```

The Challenge: Proving Compliance

Is a “Vendor Report” Acceptable Supporting Documentation ?



```
VRAAPDS1   VER 8.1                    VANGUARD ADMINISTRATOR                              PAGE       1
09009905                              DATASET PROFILE SUMMARY                             CPU   0363B4
                                  REPORT DATED: AUG 13, 2010   05:35
                              INFORMATION AS OF: AUG 13, 2010   05:30
MASKING CRITERIA: Dataset/PCI.*
SORTED BY: Profile Name in ascending order

                                                                                   Universal           Discrete Vol
           Profile Name                        Type     Owner    Creation Date  Notify  Warning  Access    Volume   Error Msg
 -------------------------------------------- -------- -------- -------------- -------- ------- --------- ------ ------------
 PCI.**                                       GENERIC  PCI      APR  8, 2010   TSJY00            NONE
 PCI.CREDIT.DATA                              DISCRETE PCI      OCT 21, 2008   TSJY00    YES     READ      VOL002
 PCI.DATA                                     GENERIC  PCI      MAY 27, 2009   TSJY00            NONE
 END OF REPORT
```

PCI Readiness Review 3Q 2010 - Confidential

Product Name

Version #

Report Name

CPU ID

“Date and Time”

Report Masking Criteria

All Profile Names

Watermark

7.2.3 Implement default “deny-all” settings

PCI.PROD.Q111.R723

RACF Readiness Reviews

A “Not in Place” Requirement = A Failed PCI Assessment

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
7.2.3 Default “deny-all” setting	7.2.3 Confirm that the access control systems has a default “deny-all” setting		Not in place	1) The dataset profile named PCI.CREDIT.DATA is not configured to support a “deny-all” setting (UACC=READ, and WARNING) 2) The “Not in Place” findings are shown in the Vanguard Administrator, Dataset Profile Report, dated August 13, 2010.

RACF Readiness Review – Example #1

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements	Testing Procedure	In Place	Not in Place	Target Date / Comments
2.1 Always change vendor supplied defaults before installing a system on the network.	2.1 Chose a sample of system components, critical servers and attempt to logon to the devices using default vendor-supplied accounts and passwords to verify that default accounts and passwords have been changed.			

RACF Readiness Review – Example #1

Supporting Documentation

```
LISTUSER  IBMUSER

 USER=IBMUSER  NAME=DEFAULT ID   OWNER=SYS1  CREATED=95.157

 DEFAULT-GROUP=SYS1  PASSDATE=95.100 PASS-INTERVAL=N/A   PHRASEDATE=N/A

 ATTRIBUTES=REVOKED

 REVOKE DATE=NONE   RESUME DATE=NONE

 LAST-ACCESS=95.100/09:29:06

 CLASS AUTHORIZATIONS=NONE
```

RACF Readiness Review – Example #1

Supporting Documentation

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
   5 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
 RULE 1  LENGTH(6:8)   LLLLLLLL
    LEGEND:
     A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
     c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

RACF Readiness Review – Example #1

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
2.1 Always change vendor supplied defaults before installing a system on the network.	2.1 Chose a sample of system components, critical servers and attempt to logon to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed.		Not in Place	1) Logged on to IBMUSER using the default password of “SYS1”, the userid was revoked. 2) The SETROPTS RVARY password is set to the vendor-supplied default. 3) The *security administrator* was observed collecting the supporting documentation on the SYSPRD system on January 14, 2010.

RACF Readiness Review – Example #2

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.9 Change user passwords at least every 90 days	8.5.9 For a sample of system components, obtain and inspect system configuration settings to verify that user passwords are set to require users to change passwords at least every 90 days.			

RACF Readiness Review – Example #2

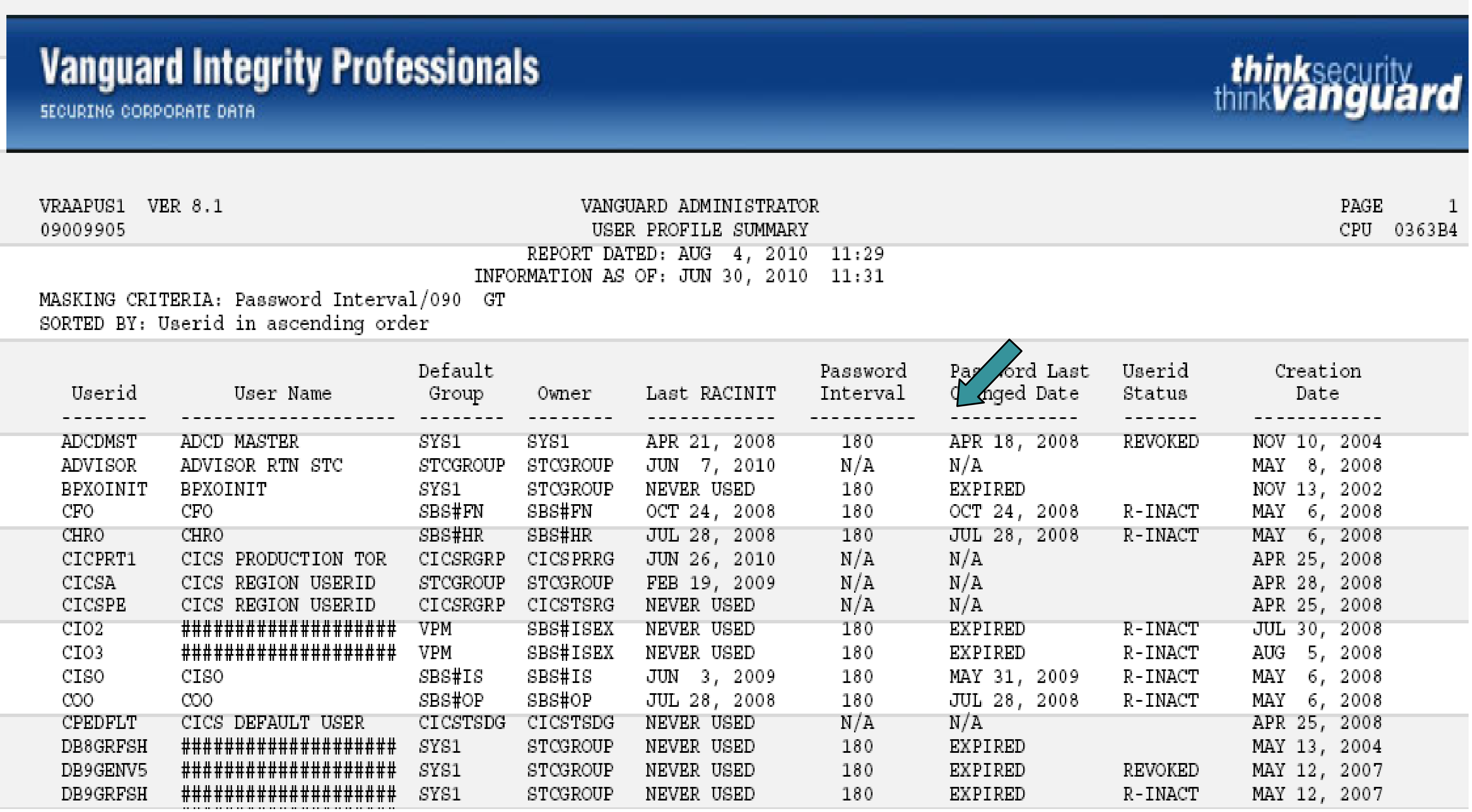
Supporting Documentation

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
   5 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
 RULE 1  LENGTH(6:8)   LLLLLLLL
    LEGEND:
     A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
     c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

RACF Readiness Review – Example #2

SHARE
Technology · Connections · Results

Supporting Documentation



Vanguard Integrity Professionals
SECURING CORPORATE DATA

thinksecurity
thinkvanguard

```
VRAAPUS1  VER 8.1                       VANGUARD ADMINISTRATOR                                   PAGE       1
09009905                                 USER PROFILE SUMMARY                                    CPU   0363B4
                                  REPORT DATED: AUG  4, 2010   11:29
                               INFORMATION AS OF: JUN 30, 2010   11:31
MASKING CRITERIA: Password Interval/090  GT
SORTED BY: Userid in ascending order

                                     Default                                Password   Password Last  Userid         Creation
  Userid          User Name           Group      Owner     Last RACINIT     Interval   Changed Date   Status           Date
 --------   --------------------   --------   --------   ------------   ----------   ------------   -------     ------------
 ADCDMST    ADCD MASTER            SYS1       SYS1       APR 21, 2008      180       APR 18, 2008   REVOKED     NOV 10, 2004
 ADVISOR    ADVISOR RTN STC        STCGROUP   STCGROUP   JUN  7, 2010      N/A       N/A                        MAY  8, 2008
 BPXOINIT   BPXOINIT               SYS1       STCGROUP   NEVER USED        180       EXPIRED                    NOV 13, 2002
 CFO        CFO                    SBS#FN     SBS#FN     OCT 24, 2008      180       OCT 24, 2008   R-INACT     MAY  6, 2008
 CHRO       CHRO                   SBS#HR     SBS#HR     JUL 28, 2008      180       JUL 28, 2008   R-INACT     MAY  6, 2008
 CICPRT1    CICS PRODUCTION TOR    CICSRGRP   CICSPRRG   JUN 26, 2010      N/A       N/A                        APR 25, 2008
 CICSA      CICS REGION USERID     STCGROUP   STCGROUP   FEB 19, 2009      N/A       N/A                        APR 28, 2008
 CICSPE     CICS REGION USERID     CICSRGRP   CICSTSRG   NEVER USED        N/A       N/A                        APR 25, 2008
 CIO2       ####################   VPM        SBS#ISEX   NEVER USED        180       EXPIRED        R-INACT     JUL 30, 2008
 CIO3       ####################   VPM        SBS#ISEX   NEVER USED        180       EXPIRED        R-INACT     AUG  5, 2008
 CISO       CISO                   SBS#IS     SBS#IS     JUN  3, 2009      180       MAY 31, 2009   R-INACT     MAY  6, 2008
 COO        COO                    SBS#OP     SBS#OP     JUL 28, 2008      180       JUL 28, 2008   R-INACT     MAY  6, 2008
 CPEDFLT    CICS DEFAULT USER      CICSTSDG   CICSTSDG   NEVER USED        N/A       N/A                        APR 25, 2008
 DB8GRFSH   ####################   SYS1       STCGROUP   NEVER USED        180       EXPIRED                    MAY 13, 2004
 DB9GENV5   ####################   SYS1       STCGROUP   NEVER USED        180       EXPIRED        REVOKED     MAY 12, 2007
 DB9GRFSH   ####################   SYS1       STCGROUP   NEVER USED        180       EXPIRED        R-INACT     MAY 12, 2007
```

SHARE in Anaheim 2011

RACF Readiness Review – Example #2

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.9 Change user passwords at least every 90 days	8.5.9 For a sample of system components, obtain and inspect system configuration settings to verify that user passwords are set to require users to change passwords at least every 90 days.		Not In Place	1) The system-level password change interval is set to 60 days. 2) Userids with non-expiring passwords exist, and are being remediated. 3) Userids with passwords greater than 90 days exist, recommendation is to reset the password intervals to 60 days.

RACF Readiness Review – Example #3

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.10 Require a minimum password length of at least seven characters	8.5.10 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.			

RACF Readiness Review – Example #3

Supporting Documentation

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
   5 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
 RULE 1  LENGTH(6:8)   LLLLLLLL
    LEGEND:
     A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
     c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

RACF Readiness Review – Example #3

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.10 Require a minimum password length of at least seven characters.	8.5.10 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords be at least seven characters long.		Not in Place	1) The system-level password rules allow new passwords to be a minimum of six characters, the requirement is a minimum of seven characters. 2) The *security administrator* was observed collecting the supporting documentation on the SYSPRD system on January 14, 2011

RACF Readiness Review – Example #4

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	8.5.12.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.			

RACF Readiness Review – Example #4

Supporting Documentation

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
   5 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
 RULE 1  LENGTH(6:8)   LLLLLLLL
    LEGEND:
     A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
     c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

RACF Readiness Review – Example #4

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	8.5.12.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.	In Place		The SETROPTS settings are set to retain 5 GENERATIONS OF PREVIOUS PASSWORDS.

RACF Readiness Review – Example #5

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	8.5.13 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that a users account is locked out after not more than six invalid logon attempts.			

RACF Readiness Review – Example #5

Supporting Documentation

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
   5 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
 RULE 1  LENGTH(6:8)   LLLLLLLL
    LEGEND:
     A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
     c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

RACF Readiness Review – Example #5

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	8.5.13 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that a users account is locked out after not more than six invalid logon attempts.	In Place		1) The SETROPTS configuration is set to limit repeated access attempts by locking out the user ID after 4 invalid attempts. 2) The security administrator was observed collecting the supporting documentation on the SYSPRD system on January 15, 2011

RACF Readiness Review Results

PCI DSS Requirements	Results
2.1 Always change vendor supplied defaults before installing a system on the network.	Not In Place
8.5.9 Change user passwords at least every 90 days	Not in Place
8.5.10 Require a minimum password length of at least seven characters	Not in Place
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	In Place
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	In Place

RACF System Hardening Standards

RACF System Hardening Standards

PCI DSS Requirement	Testing Procedure
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.
2.2.3 Configure system security parameters to prevent misuse.	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.

RACF System Hardening Standards

zOS RACF Security Technical Implementation Guide

UNCLASSIFIED

z/OS RACF STIG

Version: 6

Release: 5

29 Oct 2010

STIG.DOD.MIL

RACF0460

RACF0460 - The PASSWORD(RULEn) SETROPTS value(s) specified is/are improperly set

If the PASSWORD(RULEn) values shown under "INSTALLATION PASSWORD SYNTAX RULES" are as follows, there is NO FINDING:

RULE 1 LENGTH(8) $mmmmmmm
RULE 2 LENGTH(8) m$mmmmmm
RULE 3 LENGTH(8) mm$mmmmm
RULE 4 LENGTH(8) mmm$mmmm
RULE 5 LENGTH(8) mmmm$mmm
RULE 6 LENGTH(8) mmmmm$mm
RULE 7 LENGTH(8) mmmmmm$m
RULE 8 LENGTH(8) mmmmmmm$

If the "MIXED CASE PASSWORD SUPPORT IS IN EFFECT" is shown under "PASSWORD PROCESSING OPTIONS", there is NO FINDING.

If this is set to any other values, this is a FINDING

RACF System Hardening Standards

There is no PCI Requirement for “Mixed Case Passwords”

```
PASSWORD PROCESSING OPTIONS:
  PASSWORD CHANGE INTERVAL IS  60 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS   0 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
   5 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   6 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS  10 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
 RULE 1  LENGTH(6:8)   LLLLLLLL
    LEGEND:
     A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-
ANYTHING
     c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
 DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
```

RACF System Hardening Standards

How would you Rate this Requirement?

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirement	Testing Procedure	In Place	Not in Place	Target Date / Comments
2.2.3 Configure system security parameters to prevent misuse.	2.2.3.b Verify that common security parameter settings are included in the system configuration standards.		Not in Place	Vendor supplied defaults have not been changed, the RACF configuration standards do not include support for mixed case passwords (see STIG RACF0440 as guidance.)

Questions

VANGUARD
INTEGRITY PROFESSIONALS, INC.

enterprise security software

For additional information:

Phone Number: 702-794-0014

Website: http://www.go2vanguard.com

E-Mail: info@go2vanguard.com

jim.yurek@go2vanguard.co