# So how do I actually apply DISA STIGs to ACF2, RACF and/or TSS?

DEFENSE INFORMATION SYSTEMS AGENCY

# Agenda

- Who are DISA?
- What is a STIG?
- Security Positioning?
- Similarities between ESM STIGs
- Differences between ESM STIGs
- Where Now? RACF
- Where Now? CA ACF2
- Where Now? CA Top Secret

# Who are DISA?

- Defense Information Systems Agency
- Note the eagle...
  - US Government Department
  - So...
    - You must implement all relevant DISA STIGs if you want to do business with the US government
    - Many are choosing DISA STIGs outside of those required

# What is a STIG?

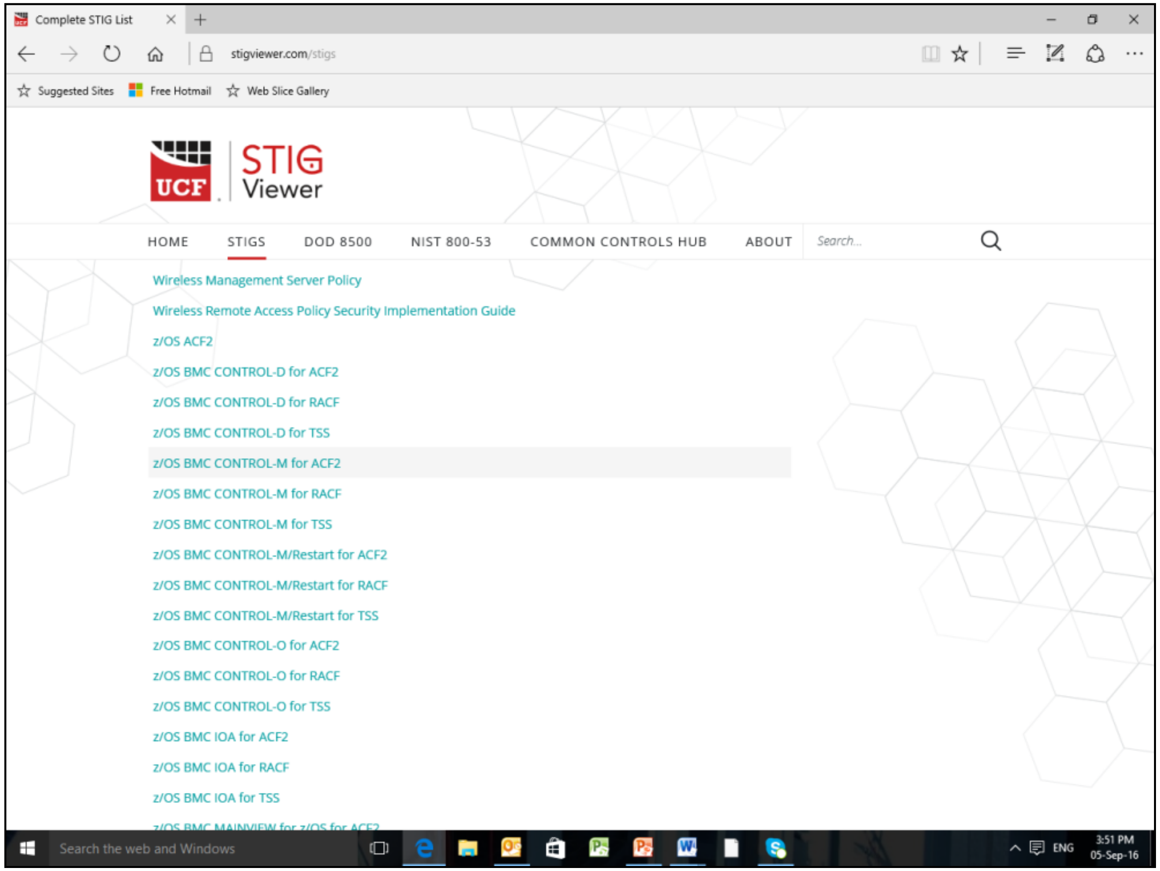
- Security Technical Information Guides
  - Documented audit points for a great many IT systems
  - The United States Department of Defense creates and maintains the DISA STIGs
  - Rapidly become the “Gold Standard for IT Security” across platforms as diverse as your mobile phone and your mainframe!

# What is a STIG?

- Security Technical Information Guides
  - “Secure RACF Implementation”
  - “Secure CA ACF2 Implementation”
  - “Secure CA TSS Implementation”
- Must use a STIG Viewer
  - https://www.stigviewer.com/stigs

# What is a STIG?

- No single view of ESM provided by DISA



Wireless Management Server Policy

Wireless Remote Access Policy Security Implementation Guide

z/OS ACF2

z/OS BMC CONTROL-D for ACF2

z/OS BMC CONTROL-D for RACF

z/OS BMC CONTROL-D for TSS

z/OS BMC CONTROL-M for ACF2

z/OS BMC CONTROL-M for RACF

z/OS BMC CONTROL-M for TSS

z/OS BMC CONTROL-M/Restart for ACF2

z/OS BMC CONTROL-M/Restart for RACF

z/OS BMC CONTROL-M/Restart for TSS

z/OS BMC CONTROL-O for ACF2

z/OS BMC CONTROL-O for RACF

z/OS BMC CONTROL-O for TSS

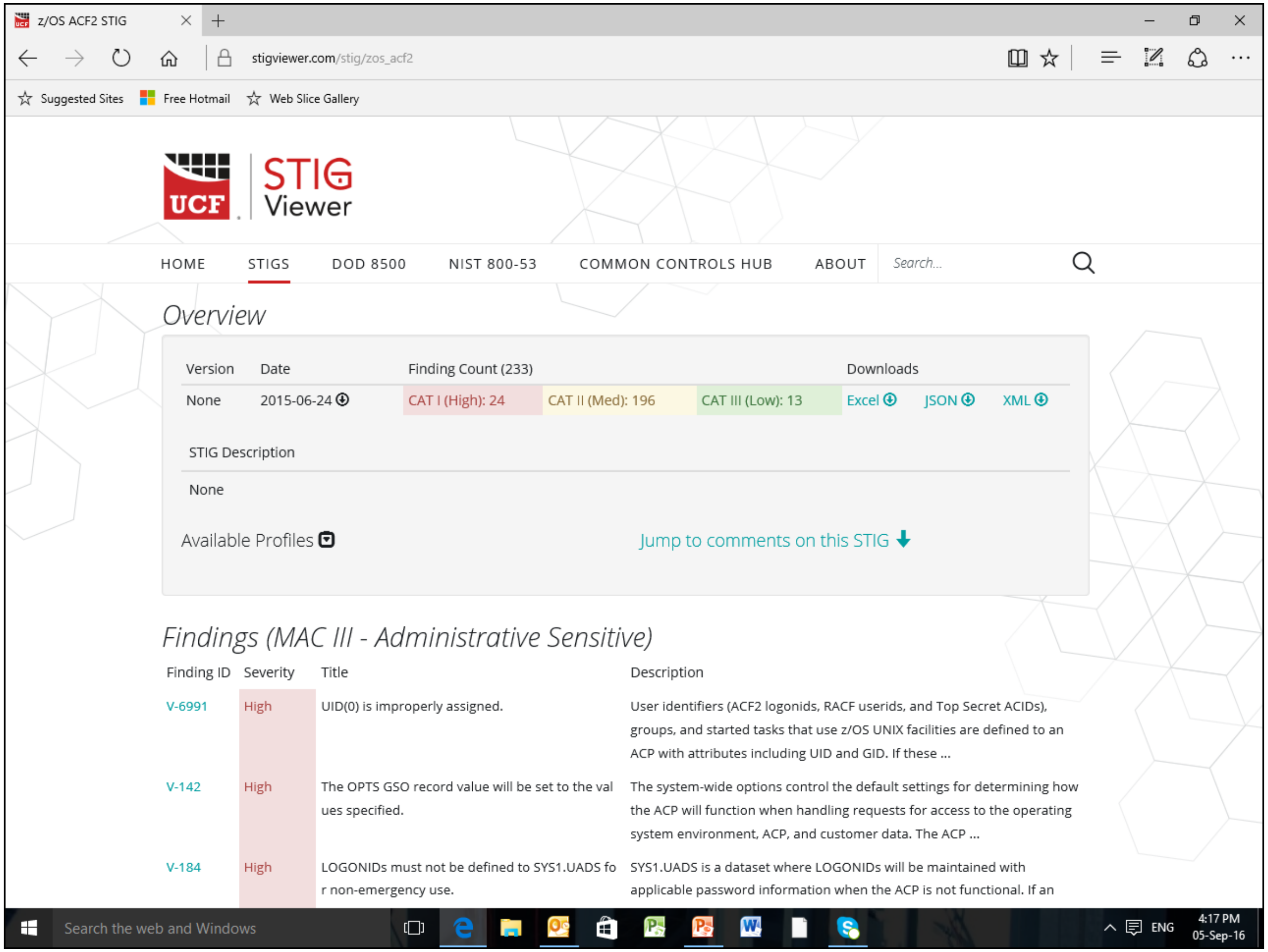
z/OS BMC IOA for ACF2

z/OS BMC IOA for RACF

z/OS BMC IOA for TSS

z/OS BMC MAINVIEW for z/OS for ACF2

# What is a STIG?



## Overview

| Version | Date | Finding Count (233) | | | Downloads | | |
|---|---|---|---|---|---|---|---|
| None | 2015-06-24 | CAT I (High): 24 | CAT II (Med): 196 | CAT III (Low): 13 | Excel | JSON | XML |

STIG Description

None

Available Profiles

Jump to comments on this STIG

## Findings (MAC III - Administrative Sensitive)

| Finding ID | Severity | Title | Description |
|---|---|---|---|
| V-6991 | High | UID(0) is improperly assigned. | User identifiers (ACF2 logonids, RACF userids, and Top Secret ACIDs), groups, and started tasks that use z/OS UNIX facilities are defined to an ACP with attributes including UID and GID. If these ... |
| V-142 | High | The OPTS GSO record value will be set to the values specified. | The system-wide options control the default settings for determining how the ACP will function when handling requests for access to the operating system environment, ACP, and customer data. The ACP ... |
| V-184 | High | LOGONIDs must not be defined to SYS1.UADS for non-emergency use. | SYS1.UADS is a dataset where LOGONIDs will be maintained with applicable password information when the ACP is not functional. If an |

# Security Positioning?

- Basic “Rules of Thumb”
  - Always educate your Users on what security means to you
  - Always have a way to find out who owns what
  - Always question requests for access
  - Never grant more access than is actually needed
  - Never grant access for longer than it is needed
  - Never stop questioning requests for access!

# Security Positioning?

- Basic “Rules of Thumb”
  - **ALWAYS** MONITOR **EVERYTHING** THAT HAPPENS ON YOUR SYSTEM!!!
  - Without an audit record, it is impossible to tell what has happened when the “Bad Guys” aka “Black Hats” get in to your system
  - Learn from the NSA : Start with the assumption that you have already been “hacked”

# Similarities between ESM STIGs

- A lot of similarities
  - All STIGs are specific to specific software environments
    - No overall view of ESM STIGs
  - Most include commands required to set options etc

# Similarities between ESM STIGs

- Password Rules
  - Increasing the size of the character sets being used for passwords results in stronger passwords as it makes it harder for hackers to gain access
  - Mixed case passwords should be used as this will greatly improve password security
  - Use of AES encryption on stored passwords makes them more secure by dramatically increasing the time and effort required to decrypt them
  - Password history should be set to 10 or higher

# Similarities between ESM STIGs

- Password Rules - RACF
  - 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$m
  - RULE 8 LENGTH(8) mmmmmmm$
- These rules represent the fact that all passwords must be 8 characters in length and contain a National character in any position with all of the other characters being Mixed Alpha Numeric

# Similarities between ESM STIGs

- Password Rules – CA ACF2
  - DISA STIGs require:
    - MINPSWD value of 8
    - PSWDALPH to be enabled
    - PSWDLC to be enabled
    - PSWDUC must be enabled
    - PSWDLID to be enabled
    - PSWDMIXD must be enabled
    - PSWDNUM must be enabled
    - value of 0 for PSWDPAIR
    - PSWDREQ must be enabled
- So do these…

# Similarities between ESM STIGs

- Password Rules – CA Top Secret.
  - The DISA STIGs dictate that **NEWPW** must be set as follows:
    - MIN=8
    - WARN=10
    - MINDAYS=1
    - NR=0
    - MC
    - UC
    - LC
    - PASSCHAR(@,#,$) (These are the minimum special characters that can be specified)
    - ID
    - TS
    - SC
    - RS
    - FA
    - FN
- And these…

# Differences between ESM STIGs

- ESM Product Design Differences
- Underlying z/OS Subsystem Differences
  - e.g. CICS vs IMS
- Rules submitted to DISA by External Agencies
  - Maybe lack of understanding
  - Maybe not yet reported
    - If you are a US Organization, you can report new findings to DISA
  - Maybe new rule set being rolled out
  - Constantly being updated

# Where now? RACF

- STIGs!
- Big 4 Audit Check Lists
- NewEra Knowledge Project
  - 83 pages

z/Auditing Essentials

Volume 1

Testing RACF – SETROPTS

[illegible]

[illegible]

[illegible]

- http://www.newera-info.com/eBooks.html

# Where now? CA ACF2

- STIGs!
- Big 4 Audit Check Lists
- NewEra Knowledge Project
  - 142 pages

z/Auditing Essentials

Volume 1

Mastering CA ACF2 – [illegible]

[illegible]

- http://www.newera-info.com/eBooks.html

# Where now? CA Top Secret

- STIGs!
- Big 4 Audit Check Lists
- NewEra Knowledge Project
  - 94 pages

z/Auditing Essentials

Volume 1

Controlling CA Top Secret

[illegible]

[illegible]

[illegible]

- http://www.newera-info.com/eBooks.html

# Thank You!

Julie-Ann Williams
Managing Director
millennia...
julie@sysprog.co.uk