

# DII COE Compliance Evaluation of Air Force Mission Applications

Presented to NTAG  
3 February, 2000

Eric L. Krum  
GCCS-AF  
MITRE  
781-271-5144  
krume@mitre.org

# Purpose

---

To provide information on the procedures and tools used by the Air Force Certification and Test Facility (AFCTF) in the DII COE compliance evaluation of Air Force NT-based mission applications

# Outline

---

- Goal
- Background
- Evaluation Outline
- Tools
- Output
- Status
- Issues
- Future
- Summary

# Goal

---

Create a standard set of procedures that

- provides consistency,
- are impartial,
- repeatable, and
- releasable to contractors

# Background

- Air Force Certification and Test Facility (AFCTF) evaluates GCCS-AF segments and segments procured by Program Offices on Hanscom AFB
- COE incorporates Windows NT Logo compliance
- Procedures required to measure compliance with DII COE I&RTS (Appendix B) & Logo
- Air Force COE segment development and compliance process defined on web site:

<http://dii-af.hanscom.af.mil/infrastructure/Implementation/default.htm>

# Process

The screenshot shows a Microsoft Internet Explorer browser window displaying the website for the Defense Information Infrastructure (DII). The page title is "Submit Application for Compliance Testing". The browser's address bar shows the URL: [https://di-hq.hanscom.af.mil/infrastructure/implementation/NO\\_FRAMES/testing.htm](https://di-hq.hanscom.af.mil/infrastructure/implementation/NO_FRAMES/testing.htm). The website header includes the DII logo and the text "Defense Information Infrastructure" and "Implementing DII-Compliant Systems". A left-hand navigation menu lists various links such as "JTS FAQ", "DII COE FAQ", "The Process", "Overview", "COE Requirements", "Register Segment", "I&RTS Waivers", "Segmentation", "Download DII COE Documentation", "Questionnaire", "Schedule Resources", "Compliance Testing", and "Raiding". The main content area features the heading "SUBMIT APPLICATION FOR COMPLIANCE TESTING" and a sub-heading "This page was last updated on: Friday, September 17, 2010". The text on the page reads: "Congratulations! If you've gotten this far in the process, and have interacted with us along the way, then you're on the home stretch! Even if your segment(s) won't be going to DISA, we still require the same documentation as DISA does for COE components and Joint applications. Assuming you've coordinated for resources (see [Scheduling page](#)) and provided us with all the information we need to put your application through the paces ([Questionnaire](#)), then you're ready to deliver your segment(s) to us." Below this, it states "Submits the package to the ESC DII AFCTF:" followed by the address: "HQ ESC/DW, Attention: Configuration Management, 6 Eglin Street, Hanscom AFB, MA 01731-2100". A section titled "Make sure the Package Includes:" lists four items: "Delivery Letter (Soft Copy) (Rich Stebbins Process Flow)", "I&RTS Waivers Granted (Soft Copy) (Julie Surer Process Flow)", "2 Copies of Segment (with Licenses) on Media for Field Delivery", and "Completed NT AFCTF Questionnaire (Soft Copy)". The Windows taskbar at the bottom shows the Start button, several application icons, and the system clock displaying 12:53 PM.

## Process (con't)

---

- Evaluate Segment Delivery for Completeness
- Review I&RTS Appendix B and Analyze.exe results
- Spot-check Analyze.exe results
- Follow Installation Procedures to install/uninstall segment
- Exercise application IAW User's and Administrator's Manuals
- Load and check other segments that will co-exist with segment under Compliance Checking
- Assign Compliance Level
- Determine areas that need to be addressed in the next version of the segment
- Prepare and deliver Report to submitting Agency (Soft Copy)
- If system/segment is qualified, prepare and deliver Certification Memo to Submitting Agency (Hard Copy)

## Background (con't)

---

- AFCTF mission:
  - Evaluate COE and Logo Program compliance
  - Assist SPOs at any point during development cycle
  - Assist developers at any point during development cycle

# Evaluation Outline

---

- Start with pristine system (30 seconds to build)
  - Windows NT 4.0
  - Current Service Pack
  - COE kernel (3.0, 3.1, 3.2, 3.3, 3.4, or 4.1)
  - Baseline applications
  - GCCS-AF Security configuration
- Follow AFCTF Segment – COE Compliance Evaluation worksheet
- Complete Evaluation Report

# COE Evaluation form (Sample)

Step #	I&RTS Ref.	T R U E	F A L S E	N / A	Step Description and Comments
34	Level 6-35 [5.10.8, p. 5-159]				<p>[All Segments] If the segment creates temporary files, they are deleted when no longer needed.</p> <ol style="list-style-type: none"> <li>1. Open file c:\Seg_Eval\<application li="" name&gt;\&lt;segment="" prefix&gt;\aftrload\evaldata\hd_delt.txt<=""> <li>2. From the Notepad application window upper left pull-down menus, select Search-Find...</li> <li>3. Type "Temp" and begin search. Hit F3 key to perform follow-on searches. If there are any files found located in the C:\Temp directory after installation, segment fails step.</li> </application></li></ol> <p><b>Note: Segments will normally create temp files under the directory /temp. These are intended for use by the segment and/or the user reference -- such as .log, .lst, .lis, .rpt files -- that are there to provide information to the user. These must be deleted when the segment is de-installed (as a minimum) and, unless they are intentionally left by the segment for use by the user, should be deleted when the segment software is finished with them. The User's Manual may provide information about files left in /temp for the user -- otherwise a subjective look at these files must be done to determine if they are needed/usable (if not then they should be deleted by the software and not left in /temp).</b></p>

# Tools

---

## Tools used to collect and analyze information:

- **Analyze.exe**, provided by Microsoft for Logo Handbook compliance (free)
- **FC.exe**, file comparison for environment variable changes (free)
- **SysDiff.exe**, takes snapshot of hard drive before and after segment is installed and uninstalled. Compare snapshots to determine changes made to platform by segment (license required)
- **AddUsers.exe**, captures User and Group account information (license required)
- **Perms.exe**, captures file and directory permissions (license required)

# Analyzer Report (Sample)

AIMNT  
Monday, October 18, 1999

---

Total New Files = 51  
Total number of new 32 bit files = 11  
Total number of new 16 bit files = 0  
Total byte count of new PE\_Win32 files = 587,776  
Total byte count of new PE\_Console files = 993,948  
Total byte count of new 32 bit files = 1,581,724  
Total byte count of new 16 bit files = 0

---

## 32 Bit Files

---

[PE\_Console] Intel            942,748 c:\program files\gccs\_af\aimnt\bin\aimnt.exe  
[PE\_Win32] Intel            16,384 c:\program files\gccs\_af\aimnt\bin\dumper.dll

Total of 32 bit files = 1,581,724

---

## 16 Bit Files

---

Total of 16 bit files = 0

---

## Files that have changed

---

10/18/99 01:03:56 PM            303 c:\h\acctgrps\sysadm\segdescrip\cpp\releasenotes  
10/18/99 03:47:19 PM            272 c:\h\cots\winnt\segdescrip\cpp\version  
10/15/99 02:52:31 PM            114 c:\seg\_eval\aimnt\aimnt\aftrload\aftrloadpath.txt  
10/18/99 03:49:31 PM            114 c:\seg\_eval\aimnt\aimnt\aftrload\aftrloadpath.txt  
10/18/99 03:47:28 PM            149 c:\winnt\coeinstaller.ini

---

## Deleted Files

## SysDiff.exe (Sample)

```
; Dump of sysdiff package c:\Seg_Eval\AIMNT\AIMNT\AFTRLOAD\SNAPDELT
; File created with sysdiff version 40006
; Sysroot: C:\WINNT
; Usrroot: C:\WINNT\Profiles\Administrator
; Usrroot: C:\WINNT\Profiles\ADMINI~1
; TotalDiffCount: 21
C:\h\AcctGrps\SysAdm\SegDescrip\cpp
    SFN: C:\h\AcctGrps\SysAdm\SEGDES~1\cpp
    Add/change ReleaseNotes (SFN: RELEAS~1)
    Add/change SegInfo
    Add/change SegName

HKLM\SOFTWARE\GCCS_AF\AIMNT\1.0.0.0
HKLM\SOFTWARE\GCCS_AF\AIMNT\CONFIG
    ftp_dir: REG_SZ/REG_EXPAND_SZ sites
    ftp_pwd: REG_SZ/REG_EXPAND_SZ segman@osf.disa.smil.mil
    ftp_target: REG_SZ/REG_EXPAND_SZ 199.114.100.117
    ftp_user: REG_SZ/REG_EXPAND_SZ anonymous
    last_ran: REG_SZ/REG_EXPAND_SZ 940276106
    schedule_day: REG_SZ/REG_EXPAND_SZ 2
```

## FC.exe (Sample)

- Path IDENTIFIED DIFFERENCES

Comparing files

C:\SEG\_EVAL\AIMNT\BASELINE\basepath.txt and  
C:\SEG\_EVAL\AIMNT\AIMNT\AFTRLOAD\AFTRLOADP  
ATH.TXT

FC: no differences encountered

- CONFIG.NT IDENTIFIED DIFFERENCES

Comparing files

C:\SEG\_EVAL\AIMNT\BASELINE\config.nt and  
C:\SEG\_EVAL\AIMNT\AIMNT\AFTRLOAD\CONFIG.NT

FC: no differences encountered

# Output

---

- Information Collected
  - **aebtdelt.txt**, autoexec.bat file changes
  - **aentdelt.txt**, autoexec.nt file changes
  - **cfntdelt.txt**, config.nt file changes
  - **cfsydelt.txt**, config.sys file changes
  - **pathdelt.txt**, PATH variable changes
  - **ENVI\_delt.txt**, system environment variable changes
  - **SERVICES.txt**, service (daemon) changes
  - **Obsolete.txt**, obsolete directory names and descriptors used
  - **permissions.txt**, illegal directory and file permissions
  - **USER\_GRP\_delt.txt**, User and Group account changes
  - **hosts\_delt.txt**, IP host changes
  - **start\_menu.txt**, menu icon changes
- Screen Shots of evaluator input and identified problems

## Output (con't)

---

- Analyzer output
  - **c-finalrpt1.doc**, C: drive file and directory information
  - **c-report1.doc**, registry and system information
- Sysdiff output
  - HD\_DELT.TXT, all changes made to platform
- Compliance Evaluation Form
- Segment Evaluation Report

# Status

---

- Segment Evaluation Report Template (100%)
- Compliance Evaluation Form (100%)
- Web site update (50%)
- Verification of tools and procedures (100%)

# Issues

---

- DISA ACAT, (ChkCompliance) automated compliance evaluation tool
- Logo evaluation
  - 36 items total
  - 27 testable
  - 9 need tests developed
- Require commercial Logo verification
- Security lockdown and unlock utilities
- Position paper on Windows 95/98
- Windows 2000 Certification Program
- Rational Certification test Suite
  - <http://www.rational.com/products/teamtest/w2k/index.jtimpl>

# Future

---

- Auto selection of compliance items for evaluation based on COE level and segment type
- Automated tools complete evaluation and auto fill compliance form
- Metrics to allow
  - Statistical analysis of compliance items
  - Tracking of compliance items by developer
  - Schedule segments based on previous time required
- Database to store results

# Summary

---

- Windows NT COE segments must be COE and Logo Program compliant
- AFCTF Lab services include:
  - Compliance evaluation
  - Program management support
  - Developer support