Compliance Self Test Plan for GENERIC, Adobe Acrobat Pro DC Continuous Track

08 DEC 2023

SIGNATURES

Information System Security Manager:

_____	_____
Name	**Date**
ISSM	

Information System Security Officer:

_____	_____
Name	**Date**
ISSO	

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

The purpose of the GENERIC Test Plan is to provide all involved parties with a discrete set of measurement and expected outcomes in order to gauge successful security compliance self-testing for the GENERIC system at the installation location. Additionally, this document will outline the resources needed to successfully accomplish this test.

1.2 Scope

The scope of this test includes the test cases for the Adobe Acrobat Professional DC Continuous Track reference to Defense Information Systems Agency (DISA) Security technical Implementation Guide (STIG) version 2, release 1, on the GENERIC baseline system.

2. Environment (Target System)

The GENERIC system is comprised of the following sub-systems with associated operating systems and Original Equipment Manufacturer (OEM) as defined;

- INSERT SYSTEM (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER]

- LIST

The interface control systems that are testable in the target system include the account consoles to the GENERIC system, as defined by access through the sub-system.

2.1 Security Environment

The security environment will be at the [INSERT LEVEL OF SECURITY] level and will require the appropriate security and control measures suitable for the data being processed. All personnel will require access authorization to both the testing facility and the data produced on the system components. Any test materials, data, or reports identified as being classified will require the appropriate markings, protection, transmission, handling and storage procedures.

3. Responsibilities

3.1 Site ISSM

Organizational personnel will provide logistical and technical support to the OEM team during the installation and test period. Support should include any system administration or network administration that must be accomplished on the host environment in order to successfully integrate the test system into the [ORGANIZATIONAL] network.

3.2 Site ISSO

Implementation of appropriate security controls to maintain information system risk and associated mission risk at an acceptable level as determined by the Authorizing Authority (AO). The system controls, the particular controls with [ORGANIZATIONAL] defined parameters in Committee on National Security Systems Instruction (CNSSI) 1253 are referenced by the following list:

- INSERT SYSTEM CONTROL (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER] [PARAMETER]

- LIST

3.3 [ORGANIZATION]

Develop the cybersecurity compliance self-test plan. The test procedures contained in this document are referenced to GENERIC Adobe Acrobat Professional DC Continuous Track system.

4. Test Execution Instructions

i) The test procedure sheet may be filled out manually or electronically.
   (1) Complete the entries for target system, date, and test representative at the beginning of the procedure.
   (2) All information assurance security controls in the table must be marked as:
      (a) Pass:
         (i) the device passed the security test
      (b) Fail:
         (i) the device failed the test; or
         (ii) device lacks the capability and is not compensated by another device/measure
      (c) Not Evaluated:
         (i) no test provided; or
         (ii) the device is not available for testing; or
         (iii) the device lacks the capability but is compensated by another device/measure
   (3) Provide comments for any control not marked as Pass.
   (4) Upon completion, the score sheet is digitized if necessary, and uploaded as an exhibit to the appropriate [ORGANIZATION] project reference.

4.1 Test Procedure

The following pages provide the detailed test procedure required to perform the target system compliance self-test plan.

Step	Step Description	Expected Results/Comments	P/F
Security Test Case TEST SCENARIO: The test executioner will log onto a [access interface] workstation and execute a series of commands and check the results against the respective expected results that are listed below. TEST SETUP: 1. The test executioner will log into a [access interface] workstation with valid LDAP user with privileged access (account should have a ".priv" at the end of it). 2. Once logged on, the test executioner will open a shell by clicking on Hosts and selecting Console. 3. Within the shell, the test execution will execute the following shell commands			
N/A	**Record Test Start Date/Time**	**Start Date:** _____ **Start Time:** _____	N/A
Test 1 CCI-001695 **Prevent the execution of organization-defined unacceptable mobile code.** **NIST SP 800-53 Revision 5 :: SC-18 (3)** **CCI-002530** **Maintain a separate execution domain for each executing system process.** **NIST SP 800-53 Revision 5 :: SC-3**			

Step	Step Description	Expected Results/Comments	P/F
1	Adobe Acrobat Pro DC Continuous Enhanced Security for standalone mode must be enabled.	Verify the following registry configuration: Utilizing the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bEnhancedSecurityStandalone Type: REG_DWORD Value: 1 If the value for bEnhancedSecurityStandalone is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Security (Enhanced) > In the 'Enhanced Security' section> Verify 'Enable Enhanced Security' checkbox is checked and greyed out (locked). If the box is not checked nor greyed out (locked), this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Security (Enhanced) > 'Enable Enhanced Security Standalone' must be set to 'Enabled'.	

Test 2 CCI-001695
Prevent the execution of organization-defined unacceptable mobile code.
NIST SP 800-53 Revision 5 :: SC-18 (3)

CCI-002530
Maintain a separate execution domain for each executing system process.
NIST SP 800-53 Revision 5 :: SC-39

Step	Step Description	Expected Results/Comments	P/F
2	Adobe Acrobat Pro DC Continuous Enhanced Security for browser mode must be enabled.	Verify the following registry configuration: Utilizing the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bEnhancedSecurityInBrowser Type: REG_DWORD Value: 1 If the value for bEnhancedSecurityInBrowser is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Security (Enhanced) > 'Enable Enhanced Security In Browser' must be set to 'Enabled'.	
Test 3 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
3	Adobe Acrobat Pro DC Continuous PDF file attachments must be blocked.	Verify the following registry configuration: Utilizing the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: iFileAttachmentPerms Type: REG_DWORD Value: 1 If the value for iFileAttachmentPerms is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Trust Manager > In the 'PDF File Attachments' section > Verify 'Allow opening of non-PDF file attachments with external applications' checkbox is unchecked and greyed out (locked). If the box is checked and not greyed out (locked), this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Trust Manager > 'Allow opening of non-PDF file attachments with external applications' must be set to 'Disabled'.	

Test 4 CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

NIST SP 800-53 Revision 5 :: CM-7 a

Step	Step Description	Expected Results/Comments	P/F
4	Adobe Acrobat Pro DC Continuous access to unknown websites must be restricted.	Verify the following registry configuration: Utilizing the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cDefaultLaunchURLPerms\ Value Name: iUnknownURLPerms Type: REG_DWORD Value: 3 If the value for iUnknownURLPerms is not set to “3” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Trust Manager > In the 'Internet Access from PDF Files outside the web browser' section > Select 'Change Settings' option > In the 'PDF Files may connect to web sites to share or get information' section, if 'Block PDF files access to all web sites' is selected and greyed out (locked), then this is not a finding. If 'Custom setting' is checked, then in the 'Default behavior for web sites that are not in the above list' section, verify the radio button 'Block access' is checked and greyed out (locked) . If the box is not checked nor greyed out, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Trust Manager > 'Access to unknown websites' must be set to 'Enabled' and 'Block access' selected in the drop down box.	

Step	Step Description	Expected Results/Comments	P/F
Test 5 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
5	Adobe Acrobat Pro DC Continuous access to websites must be blocked.	Verify the following registry configuration: Utilizing the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cDefaultLaunchURLPerms\ Value Name: iURLPerms Type: REG_DWORD Value: 1 If the value for iURLPerms is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Setting the value for iURLPerms to "0" means that a custom settings has been selected. Custom setting allows for specific websites to be used for PDF workflows. These websites must be approved by the ISSO/AO otherwise the setting must be "1" which blocks access to all websites. If the iURLPerms setting is "0" and a documented risk acceptance approving the websites is provided, this is not a finding. GUI path: Edit > Preferences > Trust Manager > In the 'Internet Access from PDF Files outside the web browser' section > Select 'Change Settings' option > In the 'PDF Files may connect to web sites to share or get information' section > Verify the radio button 'Block PDF files access to all web sites' is selected and greyed out (locked). If 'Custom setting' is checked, a documented risk acceptance approved by the ISSO/AO approving the websites must be provided and then this is not a finding.	

Step	Step Description	Expected Results/Comments	P/F
		Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Trust Manager > 'Access to websites' must be set to 'Enabled' and 'Block PDF files access to all web sites' selected in the drop down box. If 'Custom setting' is selected, a documented risk acceptance approved by the ISSO/AO approving the websites must be provided and then this is not a finding.	
Test 6 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			
6	Adobe Acrobat Pro DC Continuous must be configured to block Flash Content.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bEnableFlash Type: REG_DWORD Value: 0 If the value for bEnableFlash is not set to “0” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > 'Enable Flash' must be set to 'Disabled'.	
Test 7 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
7	The Adobe Acrobat Pro DC Continuous Send and Track plugin for Outlook must be disabled.	Verify the following registry configuration: Note: The Key Name "cCloud" is not created by default in the Acrobat Pro DC install and must be created. Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cCloud Value Name: bAdobeSendPluginToggle Type: REG_DWORD Value: 1 If the value for bAdobeSendPluginToggle is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > 'Send and Track plugin' must be set to 'Disabled'.	
Test 8 CCI-001813 **Enforce access restrictions using organization-defined mechanisms.** **NIST SP 800-53 Revision 5 :: CM-5 (1) (a)**			

Step	Step Description	Expected Results/Comments	P/F
8	Adobe Acrobat Pro DC Continuous privileged file and folder locations must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bDisableTrustedFolders Type: REG_DWORD Value: 1 If the value for bDisableTrustedFolders is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Security (Enhanced) > In the 'Privileged Locations' section, verify 'Add Folder Path' option is greyed out (locked). If this option is not greyed out, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Security (Enhanced) > 'Privileged folder locations' must be set to 'Disabled'.	

Test 9 CCI-002470

Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

NIST SP 800-53 Revision 5 :: SC-23 (5)

Step	Step Description	Expected Results/Comments	P/F
9	Adobe Acrobat Pro DC Continuous periodic downloading of Adobe European certificates must be disabled.	Verify the following registry configuration: Note: The Key Name "cEUTLDownload" is not created by default in the Acrobat Pro DC install and must be created. Using the Registry Editor, navigate to the following: HKEY_CURRENT_USER\Software\Adobe\Adobe Acrobat\DC\Security\cDigSig\cEUTLDownload Value Name: bLoadSettingsFromURL Type: REG_DWORD Value: 0 If the value for bLoadSettingsFromURL is not set to “0” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Trust Manager > In the 'Automatic European Union Trusted Lists (EUTL) updates' section > Verify the 'Load trusted certificates from an Adobe EUTL server' is not checked. If the box is checked, this is a finding. Admin Template path: User Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Trust Manager > 'Load trusted certificates from an Adobe EUTL server' must be set to 'Disabled'.	
Test 10 CCI-002530 **Maintain a separate execution domain for each executing system process.** **NIST SP 800-53 Revision 5 :: SC-39**			

Step	Step Description	Expected Results/Comments	P/F
10	Adobe Acrobat Pro DC Continuous Protected Mode must be enabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bProtectedMode Type: REG_DWORD Value: 1 If the value for bProtectedMode is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > 'Protected Mode' must be set to 'Enabled'.	
Test 11 CCI-002530 **Maintain a separate execution domain for each executing system process.** **NIST SP 800-53 Revision 5 :: SC-39**			

Step	Step Description	Expected Results/Comments	P/F
11	Adobe Acrobat Pro DC Continuous Protected View must be enabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: iProtectedView Type: REG_DWORD Value: 2 If the value for iProtectedView is not set to “2” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Security (Enhanced) > In the 'Protected View' section, verify the radio button for 'All files' is checked and greyed out (locked). If the button is not checked nor greyed out, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > Security (Enhanced) > 'Protected View' must be set to 'Enabled' and 'All files' selected in the drop down box.	

Test 12 CCI-002605

Install security-relevant software updates within an organization-defined time period of the release of the updates.

NIST SP 800-53 Revision 5 :: SI-2 c

Step	Step Description	Expected Results/Comments	P/F
12	The Adobe Acrobat Pro DC Continuous latest security-related software updates must be installed.	Open Adobe Acrobat Pro DC. Navigate to and click on Help >> About Adobe Acrobat Pro DC. Verify that the latest security-related software updates by Adobe are being applied. If the latest security-related software updates by Adobe are not being applied, this is a finding.	
Test 13 CCI-001499 **Limit privileges to change software resident within software libraries.** **NIST SP 800-53 Revision 5 :: CM-5 (6)**			

Step	Step Description	Expected Results/Comments	P/F
13	Adobe Acrobat Pro DC Continuous Default Handler changes must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bDisablePDFHandlerSwitching Type: REG_DWORD Value: 1 If the value for bDisablePDFHandlerSwitching is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > General > Verify the 'Select As Default PDF Handler' option is greyed out (locked). If the option is not greyed out, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > General > 'Disable PDF handler switching' must be set to 'Enabled'.	

Test 14 CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

NIST SP 800-53 Revision 5 :: CM-7 a

Step	Step Description	Expected Results/Comments	P/F
14	Adobe Acrobat Pro DC Continuous must disable the ability to store files on Acrobat.com.	Verify the following registry configuration: Note: The Key Name "cCloud" is not created by default in the Acrobat Pro DC install and must be created. Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cCloud Value Name: bDisableADCFileStore Type: REG_DWORD Value: 1 If the value for bDisableADCFileStore is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > 'Store files on Adobe.com' must be set to 'Disabled'.	

Test 15 CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

NIST SP 800-53 Revision 5 :: CM-7 a

Step	Step Description	Expected Results/Comments	P/F
15	Adobe Acrobat Pro DC Continuous Cloud Synchronization must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cServices Value Name: bTogglePrefsSync Type: REG_DWORD Value: 1 If the value for bTogglePrefsSync is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > 'Cloud Synchronization' must be set to 'Disabled'.	
Test 16 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
16	Adobe Acrobat Pro DC Continuous Repair Installation must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: For 32 bit: HKEY_LOCAL_MACHINE\Software\Adobe\Adobe Acrobat\DC\Installer For 64 bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Adobe\Adobe Acrobat\DC\Installer Value Name: DisableMaintenance Type: REG_DWORD Value: 1 If the value for DisableMaintenance is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Help > Verify the option 'Repair Installation' is greyed out (locked). If the option is not greyed out, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > Help > 'Repair Installation on 32/64 bit' must be set to 'Disabled'.	

Test 17 CCI-000381

Configure the system to provide only organization-defined mission essential capabilities.

NIST SP 800-53 Revision 5 :: CM-7 a

Step	Step Description	Expected Results/Comments	P/F
17	Adobe Acrobat Pro DC Continuous third-party web connectors must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cServices Value Name: bToggleWebConnectors Type: REG_DWORD Value: 1 If the value for bToggleWebConnectors is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > 'Third-party web connectors' must be set to 'Disabled'.	
Test 18 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
18	Adobe Acrobat Pro DC Continuous Webmail must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cWebmailProfiles Value Name: bDisableWebmail Type: REG_DWORD Value: 1 If the value for bDisableWebmail is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > 'WebMail' must be set to 'Disabled'.	
Test 19 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
19	The Adobe Acrobat Pro DC Continuous Welcome Screen must be disabled.	Verify the following registry configuration: Note: The Key Name "cWelcomeScreen" is not created by default in the Acrobat Pro DC install and must be created. Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cWelcomeScreen Value Name: bShowWelcomeScreen Type: REG_DWORD Value: 0 If the value for bShowWelcomeScreen is not set to “0” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > 'Welcome Screen' must be set to 'Disabled'.	
Test 20 CCI-000381 **Configure the system to provide only organization-defined mission essential capabilities.** **NIST SP 800-53 Revision 5 :: CM-7 a**			

Step	Step Description	Expected Results/Comments	P/F
20	Adobe Acrobat Pro DC Continuous SharePoint and Office365 access must be disabled.	NOTE: If configured to an approved DoD SharePoint Server, this is NA. Verify the following registry configuration: Note: The Key Name "cSharePoint" is not created by default in the Acrobat Pro DC install and must be created. Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown\cSharePoint Value Name: bDisableSharePointFeatures Type: REG_DWORD Value: 1 If the value for bDisableSharePointFeatures is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: Computer Configuration > Administrative Template > Adobe Acrobat Pro DC Continuous > Preferences > 'SharePoint and Office 365 access' must be set to 'Disabled'.	
Test 21 CCI-002470 **Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.** **NIST SP 800-53 Revision 5 :: SC-23 (5)**			

Step	Step Description	Expected Results/Comments	P/F
21	Adobe Acrobat Pro DC Continuous Periodic downloading of Adobe certificates must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_CURRENT_USER\Software\Adobe\Adobe Acrobat\DC\Security\cDigSig\cAdobeDownload Value Name: bLoadSettingsFromURL Type: REG_DWORD Value: 0 If the value for bLoadSettingsFromURL is not set to “0” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Trust Manager > In the 'Automatic Adobe Approved Trust List (AATL) Updates' section > verify the 'Load trusted certificates from an Adobe AATL server' is not checked. If the box is checked, this is a finding. Admin Template path: User Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Trust Manager > 'Load trusted certificates from an Adobe AATL server' must be set to 'Disabled'.	
Test 22 CCI-001813 **Enforce access restrictions using organization-defined mechanisms.** **NIST SP 800-53 Revision 5 :: CM-5 (1) (a)**			

Step	Step Description	Expected Results/Comments	P/F
22	Adobe Acrobat Pro DC Continuous privileged host locations must be disabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Adobe Acrobat\DC\FeatureLockDown Value Name: bDisableTrustedSites Type: REG_DWORD Value: 1 If the value for bDisableTrustedSites is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. GUI path: Edit > Preferences > Security (Enhanced) > In the 'Privileged Locations' section, verify 'Add Host' option is greyed out (locked). If the option is not greyed out, this is a finding. Admin Template path: Computer Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > Security (Enhanced) > 'Privileged host locations' must be set to 'Disabled'.	

Test 23 CCI-002450

Implement organization-defined types of cryptography for each specified cryptography use.

NIST SP 800-53 Revision 5 :: SC-13 b

Step	Step Description	Expected Results/Comments	P/F
23	Adobe Acrobat Pro DC Continuous FIPS mode must be enabled.	Verify the following registry configuration: Using the Registry Editor, navigate to the following: HKEY_CURRENT_USER\Software\Adobe\Adobe Acrobat\DC\AVGeneral Value Name: bFIPSMode Type: REG_DWORD Value: 1 If the value for bFIPSMode is not set to “1” and Type is not configured to REG_DWORD or does not exist, this is a finding. Admin Template path: User Configuration > Administrative Templates > Adobe Acrobat Pro DC Continuous > Preferences > 'Enable FIPS' must be set to 'Enabled'.	

Step	Step Description	Expected Results/Comments	P/F
Notes:			

4.2 Reporting

A final After Action Report (AAR) will be provided to all [ORGANIZATION] stakeholders within 30 days of completion of demonstration execution.