ADOBE ACROBAT PROFESSIONAL (PRO) XI SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

26 January 2018

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

1. INTRODUCTION

1.1 Executive Summary

The Adobe Acrobat Professional XI Security Technical Implementation Guide (STIG) was written for the full version of Adobe Acrobat Professional with default installation parameters. Adobe Acrobat Professional XI is software used for creating, editing, and printing Portable Document Format (PDF) files. Adobe Acrobat Professional XI provides some limited access to Adobe's document cloud and online services as a precursor to features offered in Adobe Acrobat DC. Custom installations and deployments for mobile platforms such as Android and iOS are not covered in the guidance.

The Adobe Acrobat Professional XI STIG is intended to be applied to a Windows desktop environment and is published as a tool to improve the security of Department of Defense (DoD) information systems. This document is meant for use in conjunction with the Windows Operating System (OS) STIG and any appropriate STIG(s) applicable to the system.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor’s proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

2. REFERENCE DOCUMENTS

The following table enumerates documents and resources referenced:

Table 2-1: Reference Documentation

Document Description	Source
Application Security Overview	http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html
Enterprise Administration Guide	http://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/index.html
Identifying Existing Installs of Adobe Products	http://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/identify.html

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Operational View

Adobe Acrobat Professional XI is software that can be used for creating, viewing, and printing PDF documents. Adobe Acrobat Professional XI was the first to make limited use of Adobe's cloud services capabilities. The cloud capabilities in version XI introduce a potential data security risk to the DoD infrastructure, and STIG settings restrict DoD users from accessing non-DoD cloud storage resources.

Adobe Acrobat Professional XI provides a Protected Mode and Protected View configuration. Protected Mode transparently protects users against attacks by sandboxing the application processes. This allows features and functions such as scripts embedded in a PDF document to run in a restricted environment while protecting the underlying system. Protected View is a "super-sandbox" that provides a more restrictive sandbox than Protected Mode. When enabled, Acrobat will restrict the execution environment of untrusted PDFs and the processes the scripts embedded within the PDF may invoke. The user can still view the document but will be notified that some features of the document have been disabled. The STIG enables both of these modes.

The Enhanced Security setting hardens the application against additional actions that could be executed by malicious PDF files. It prevents cross-domain access; prohibits script and data injection; and blocks stream access to XObjects, silent printing, and execution of high-privilege JavaScript. Enhanced Security can be configured in two modes: Standalone mode is when Acrobat opens the desktop PDF client, and Browser mode is when a PDF is opened via the browser plugin. The STIG enables both of the Standalone and Browser mode protections.

Trusted or privileged locations provide the ability to bypass some security restrictions configured by the STIG via the yellow message bar, which prompts the user to trust the document. Trusted locations are composed of sites and servers and can also be certificate based. The STIG restricts the end user's ability to create trusted locations directly; however, system administrators or ISSOs/ISSMs may decide to establish trusted locations so as to provide trusted executable PDF content while protecting endpoints from untrusted content available on the Internet.

Issues regarding content creation and content distribution, such as signing documents, redaction procedures, or using Acrobat Pro XI workflow features, are not within the scope of the STIG and will be addressed by relevant STIGs and policy guidance that is applicable to data management and classification processes.