IBM ASPERA PLATFORM 4.2
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 2

24 August 2022

Developed by IBM and DISA for the DoD

Trademark Information

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

1. INTRODUCTION

1.1 Executive Summary

The IBM Aspera Platform 4.2 Security Technical Implementation Guide (STIG) 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 other STIGs, such as the Red Hat Enterprise Linux 7 STIG and appropriate networking and database STIGs.

1.2 Authority

Department of Defense Instruction (DoDI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures." The instruction tasks that 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 [National Security Agency/Central Security Service], 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 must 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

Category	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 DoD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.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 Controlled Unclassified Information (CUI) will be available for 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 AO. 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 DoD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DoD architecture.

2. ASSESSMENT CONSIDERATIONS

2.1 Security Assessment Information

The IBM Aspera Platform 4.2 STIG is based on the installation media for a Red Hat Enterprise Linux 7 install. Therefore, many of the requirements in the STIG are written for the RHEL command line.

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 IBM Aspera FASP protocol

Included in all IBM Aspera software and hosted services, the patented Aspera FASP protocol offers built-in security for data transfers using the standard open-source OpenSSL toolkit. The OpenSSL cryptographic library is used without modification in order to take full advantage of standards-based best practices implementation.

The IBM Aspera Platform 4.2 STIG enforces each transfer session to establish a secure control-channel that exchanges a randomly-generated per-session key for data encryption and secure authentication of the transfer endpoints. In addition, the Aspera FASP protocol provides on-the-fly data encryption, and integrity verification for each transmitted datagram.

3.2 IBM Aspera High Speed Transfer Server (HSTS)

The IBM Aspera HSTS is a remote endpoint that accepts authenticated connections from Aspera client applications and that participates as a source or destination for authorized transfers. The user's server can also take the role of a client and connect to other Aspera servers to initiate transfers.

3.3 IBM Aspera High Speed Transfer Endpoint (HSTE)

The IBM Aspera HSTE is a remote endpoint that accepts a single authenticated connection from Aspera client applications and that participates as a source or destination for authorized transfers. The user's server can also take the role of a client and connect to other Aspera servers to initiate transfers.

3.4 IBM Aspera Console

The IBM Aspera Console is a web-based administration application that provides visibility over your Aspera high-speed transfer environment, enables centralized control over transfers, nodes and users, and maintains logging for customized reports and auditing.

3.5 IBM Aspera Shares

IBM Aspera Shares is a web application that provides a way for companies to share content in the form of files and directories, of any size, within their organization or with external customers and partners. Accessible from a standard web browser, Aspera Shares provides secure access to a consolidated view of all available data content from multiple server nodes across diverse infrastructures. This is an optional feature.

3.6 IBM Aspera Faspex

IBM Aspera Faspex is a web application for file collaboration and exchange. It provides a way for individuals and groups to transfer files and directories at high-speed, regardless of size, transfer distance, or network conditions. This is an optional feature.