

UNCLASSIFIED



REMOVABLE STORAGE AND EXTERNAL CONNECTIONS SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 1, Release 7

27 October 2017

Developed by DISA for the DoD

UNCLASSIFIED

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
1. INTRODUCTION.....	1
1.1 Executive Summary	1
1.2 Authority	2
1.3 Vulnerability Severity Category Code Definitions	2
1.4 STIG Distribution.....	3
1.5 Document Revisions	3
1.6 Other Considerations	3
1.7 Product Approval Disclaimer.....	4
2. TECHNOLOGY OVERVIEW.....	5
2.1 USB Devices	5
2.1.1 USB Standards.....	5
2.1.2 USB Compliance Testing	6
2.2 Volatile and Persistent Memory Devices	7
2.3 Flash Media Use in DoD.....	8

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	3
Table 2-1: Current USB Standards	5

LIST OF FIGURES

	Page
Figure 2-1: USB Logos	7

1. INTRODUCTION

1.1 Executive Summary

This Removable Storage and External Connection Technologies Security Technical Implementation Guide (STIG) provides guidance for secure configuration and usage of removable storage media and the ports used to attach these devices to the endpoint. This document is meant for use in conjunction with other applicable STIGs such as the Wireless STIG and the appropriate operating system (OS) STIGs.

Removable storage primarily includes flash media devices (such as memory sticks, thumb drives, and camera memory cards) and external hard disk drives. These devices are typically connected to the endpoint using a high-speed external connection technology such as the Universal Serial Bus (USB) port. This STIG also implements the minimum requirements for use of USB thumb drives and is not meant to supersede or contradict the United States Cyber Command (USCYBERCOM) *Communications Task Order (CTO) 10-084 Removable Flash Media Device Implementation within and between Department of Defense (DoD) Networks*, dated 20 October 2010 (U/FOUO) or any superseding CTOs.

Although the current focus is on the USB standard, the security policies within this STIG apply to other external high-speed bus connection technologies. This STIG, therefore, also provides minimum guidance for electrically hot swappable, dynamically configurable ports and attached devices, such as Institute of Electrical and Electronics Engineers Incorporated (IEEE) 1394 (FireWire); Personal Computer Memory Card International Association (PCMCIA)/CardBus; and External Serial Advanced Technology Attachment (eSATA). Removable storage and other devices connected to external ports on the endpoint will also comply with the requirements of this STIG.

Interpretation of the CTO and STIG must be done with great care. This guidance addresses many disparate devices. The CTO addresses flash media only. Some CTO restrictions (e.g., the encryption and authentication requirements) apply only to USB thumb drives rather than to all flash media devices (e.g., camera memory cards). Additionally, many of the restrictions are not applicable to public releasable data. However, this STIG has a broader mission in that it addresses all removable storage devices and the external connections with which they attach to endpoint devices. This document supersedes *Universal Serial Bus (USB) Checklist for Sharing Peripherals across the Network, Version 1, Release 1.3*, dated 19 December 2008.

DoD Directive (DoDD) 8500.1 requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks Defense Information Systems Agency (DISA) to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DoDD 8500.1.

Although the use of the principles and guidelines in this STIG provide an environment that contributes to the security requirements of DoD systems operating at Mission Assurance Categories (MACs) I through III, applicable DoD Instruction (DoDI) 8500.2 Information Assurance (IA) controls need to be applied to all systems and architectures.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The ISSO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance. The Cyber Command (CYBERCOM) has also established requirements (i.e., timelines) for training, verification, installation, and progress reporting. These guidelines can be found on their web site: <https://www.cybercom.mil>.

Initially, these directives are discussed and released as Warning Orders (WARNORDs) and feedback to USCYBERCOM is encouraged. USCYBERCOM may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks. These requirements are designed to assist Information Security System Managers (ISSMs), ISSOs, and SAs with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

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 provide 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 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.

1.6 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 configurations 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% 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.

1.7 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 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. TECHNOLOGY OVERVIEW

This section provides background information on the USB standard and discusses general security considerations involved with using this technology.

2.1 USB Devices

USB is a serial bus standard for connecting peripherals to a host. This standard allows connection of peripherals using a single standardized interface. USB also improves plug-and-play capabilities by allowing connection and removal of devices without requiring a reboot of the endpoint. This bus can connect devices including mice, keyboards, gaming controllers, scanners, digital cameras, printers, digital media players, flash drives, and external hard drives. USB has become the standard connection method for the majority of consumer electronic devices. To date, billions of these devices have been introduced into the consumer electronics market.

USB is the first cross-platform “hot-swappable” interface. Previous interfaces, such as serial and parallel connections, required a fairly advanced knowledge of configuring Digital In-line Package (DIP) switches and Interrupt Request (IRQ) settings. Newer methods, such as Personal System 2 (PS/2), were improved but were not hassle-free and nothing compares to the nightmare known as Small Computer System Interface (SCSI) configuration.

Today’s standards support cross-platform compatibility for Macintosh, Linux/UNIX, and all versions of Windows since 98SE. These OSs include device drivers; thus, many devices do not require installation Compact Discs (CDs) or any action from the user for installation. Some devices also feature self-contained drivers so they can essentially install themselves. This convenience presents a security risk in that users do not need special knowledge or administrative rights to install and use an unauthorized USB device. There have been security incidents caused by malware or spyware which were embedded in the firmware or installed as files of some USB devices. The Removable Storage and External Connection Technologies STIG provides the minimum security requirements needed to mitigate the risks presented by the use of these devices.

2.1.1 USB Standards

Table 2-1 depicts the current USB standards and how they are used.

Table 2-1: Current USB Standards

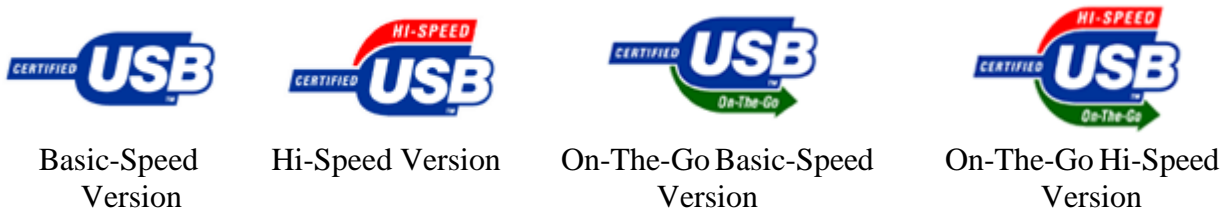
USB Standard	Definition
USB 1.x	The original implementation of USB and superseded by Release 2.0. Release 2.0 allows for additional transmission speed while maintaining backwards compatibility for USB 1.0 devices and systems.
USB 2.0 (Hi-Speed USB)	The USB 2.0, also known as the Hi-Speed USB, specification was released in 2000 and was standardized by the USB Integrator’s Forum, Inc. (USB-IF) in 2001. Several companies led the initiative to develop a higher data transfer rate of 480 Megabits per Second (Mbps), about 40 times faster than the 1.1 specification. USB 2.0 expanded the range of external devices that could be used on a computer and offered backward compatibility with previous generations.

USB Standard	Definition
USB On-the-Go supplement	<p>Many USB devices are portable, and there is an increasing need for devices to communicate directly with each other without a computer. The USB On-The-Go supplement makes it possible for peripherals to communicate directly with each other.</p> <p>USB On-The-Go supplement features include:</p> <ul style="list-style-type: none"> – Limited host capability to communicate with selected USB peripherals – A small connector appropriate for the mobile form – Low power requirements for preserving battery life – Ability to be either host or peripheral and to dynamically switch between the two
Wireless USB (WUSB)	<p>WUSB is a short-range, high-bandwidth wireless radio communication technology. The wireless architecture allows up to 127 devices to connect directly to a host. With the elimination of wires, a hub is not needed. An upcoming Wireless 1.1 specification will increase data transfer speed to 1.0 Gigabytes per Second (Gbps). It can be used in devices such as game controllers, printers, scanners, digital cameras, digital music players, hard disks, and flash drives. It can also transfer parallel video streams.</p>
USB 3.0 (SuperSpeed USB)	<p>USB 3.0, also known as SuperSpeed USB, delivers transfer rates that are up to 10 times faster than USB 2.0 through the utilization of a 5.0 Gbps data rate. Additionally, it has optimized power efficiency, sync-n-go technology that minimizes user wait-time, and backward compatibility with USB 2.0. USB 3.0 devices inter-operate with USB 2.0 platforms and the USB 3.0 hosts support Hi-Speed legacy devices.</p>

2.1.2 USB Compliance Testing

For a company to use a USB logo, its product must be compliant as demonstrated by passing the Compliance Test Program. Companies must also execute a Trademark License Agreement to be eligible for logo use. When a certified logo appears on a product, consumers know the product has passed the standards set by the standards body.

Figure 2-1 depicts the various forms of the USB official logo. Organizations should look for this logo when purchasing USB products to ensure products used within the DoD use standard protocols to the greatest extent possible.

Figure 2-1: USB Logos

Source: <http://www.usb.org/developers/compliance/logo/>

2.2 Volatile and Persistent Memory Devices

For the purpose of this Removable Storage and External Connection Technologies STIG Overview, USB devices can be divided into two categories: volatile and persistent memory devices. These categories are differentiated by the memory they contain. There are devices that contain only volatile memory or no memory at all, and there are devices that contain persistent (or non-volatile) memory.

Devices that contain volatile memory use the memory for temporary storage such as page buffers in printers, image buffers in scanners, or cache buffers in removable storage devices like Zip drives. Special notice should be made for USB hubs as they contain memory buffers even though it is not obvious. When the power is removed from these devices by unplugging them from the USB port and unplugging them from a separate power supply if one is needed, their memory is erased. Because these devices are designed to withstand minor fluctuations in power, they contain some means of maintaining memory for short power interruptions. Users need to ensure that USB devices remain without power for at least 60 seconds when disconnecting them from one Information System (IS) and connecting them to a different IS to make sure enough time passes for all power to dissipate and the memory has erased.

Devices with persistent (or non-volatile) memory will maintain the data written to them for an extended time without external power being supplied to the device. With some devices, such as hard disk drives and flash memory, the data will be maintained for the life of the device unless actions are taken to erase them. These devices include hard disk drives, flash memory (jump) drives, some Motion Picture Expert Group (MPEG) Level 1 and Layer 3 (MP3) players, battery-backed random access memory (RAM) cards, and personal digital assistants (PDAs).

Additionally, devices such as some digital cameras also contain persistent memory. Persistent memory devices do not include devices that have removable media like flash card readers, Zip drives, CD writers, and Digital Video Disk (DVD) writers (all flavors). With these devices, it is the media that is of concern, not the device. If there is any question about whether a device contains persistent memory, it should be treated as if it does until proven otherwise.

Camcorders, MP3 recording and playback devices, smart phones, and digital cameras are commonly available for official use. These devices are often treated as mass storage devices by the OS with which they are used. They represent a risk of being overlooked as persistent memory storage devices. When used to support official mission requirements, these devices must meet the security requirements for persistent memory USBs. Personal devices are often vectors for malicious code and

can be used to exfiltrate official information. These personal persistent memory devices should not be connected to an official IS without prior approval by the Authorizing Official (AO) or the designated Flash Drive Approval Authority.

2.3 Flash Media Use in DoD

In November 2008, use of flash media (e.g., memory sticks, thumb drives, and camera memory cards) with the Windows OSs was suspended throughout the DoD. Limited use of flash media devices has been restored but is severely restricted. Security policies have been added to the STIG in support of USCYBERCOM CTO 10-084 (or latest revision of this CTO). The CTO addresses minimum requirements for limited use of removable flash media devices for essential operations with systems used for direct or indirect connection to the Global Information Grid (GIG).

A USB flash drive is a flash memory data storage device that connects to the host using a USB interface. Flash memory is a persistent memory computer storage technology that can be electrically erased and reprogrammed. It is a memory chip that is primarily used in memory cards and in USB flash drives for general storage and transfer of data between computers and other digital products. The chip uses a specific type of Electrically Erasable Programmable Read-Only Memory (EEPROM) that is erased and programmed in large blocks. USB flash drives are removable and rewritable. It maintains stored information without requiring a power source. This storage method has many advantages over a traditional hard drive. There are no moving parts so drives using this technology are silent, have a smaller footprint than traditional hard drives, are highly portable, and have a faster access time.