Managing Enterprise Cybersecurity MIS 4596

Physical Security

Unit #17

Agenda

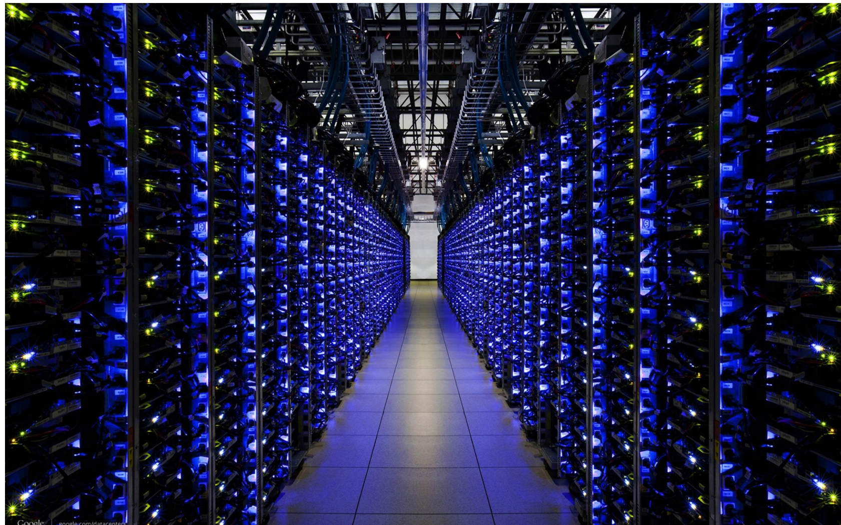
- Vulnerabilities and sources of threats
- Physical control inventory baselines
- Perimeter security
- Media protection
- Media sanitization

Physical and Environmental (PE) Security

…encompasses protection of physical assets from damage, misuse, or theft

- **Physical security addresses**
  - **…mechanisms used to create secure areas around hardware**

- **Environmental security addresses**
  - **…safety of assets from damage from environmental concerns**



Sources of physical security threats…

Materials

- ***Water*** *– floods, leaks*
- ***Chemicals and particulates -*** *smoke, toxic materials, industrial pollution*
- ***Organism*** *- virus, bacteria, animal, insect*
- *…*

Energy

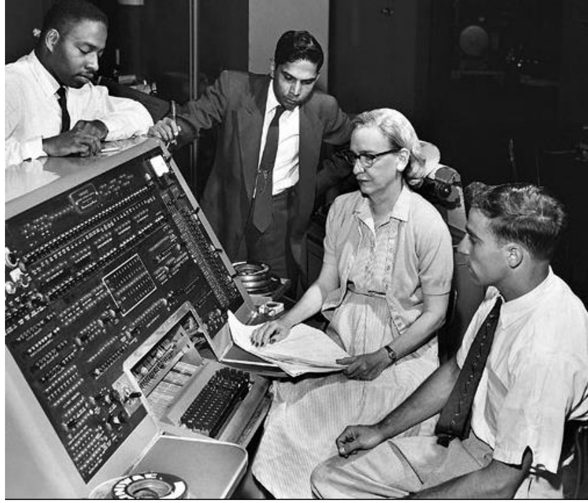
Humans

Water damage

- Damage from liquids (in general) can occur from many sources including:
  - Leaking roofs
  - Pipe breakage
  - Firefighting efforts
  - Spilled drinks
  - Flooding
  - Tsunamis

- Wet electrical equipment and computers are a lethal hazard
- **Preventative and detective controls** are necessary to make sure uncontrolled water does not destroy expensive assets or disrupt business operations
  - **Water diversion** barriers to prevent water from entering sensitive areas
  - **Water detection sensors and alarms** to detect presence of water and alert personnel in-time to prevent damage

First computer “bug”



Grace Hopper Ph.D. an American computer scientist and United States Navy rear admiral. Pioneer of computer programming, was the first to devise the theory of machine-independent programming languages, this theory was extended to create COBOL, an early high-level programming language still in use today

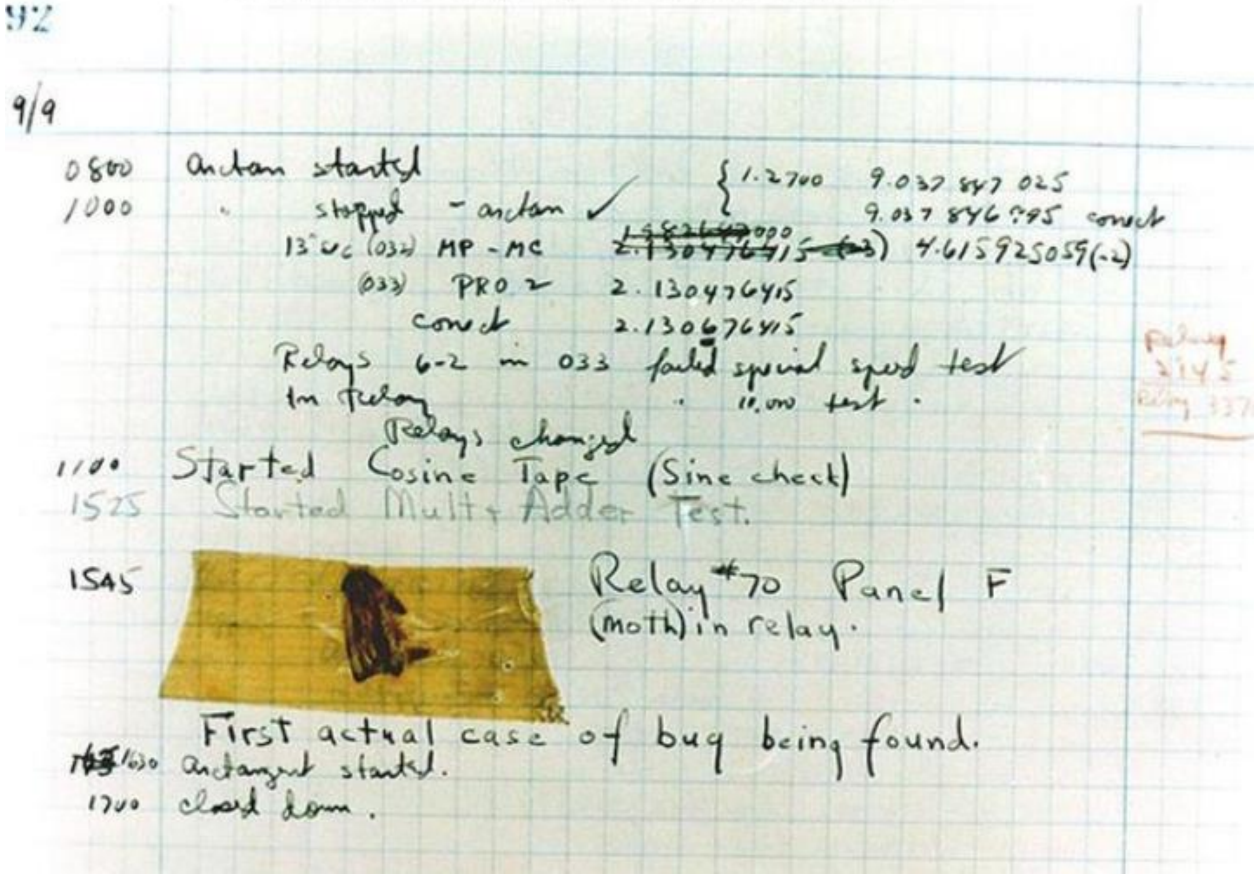
1947 Grace Hopper recorded 'the first computer bug' in the Harvard Mark II computer's log book

“First actual case of bug being found”

The problem was traced to a moth stuck between relay contacts in the computer:

- The engineers who found the moth were the first to literally "debug" a machine

Photo # NH 96566-KN (Color) First Computer “Bug”, 1947



92

9/9

0800 arctan started
1000 " stopped - arctan ✓ {1.2700 9.037 847 025
9.037 846 995 correct
13" UC (032) MP - MC ~~1.982147000~~ ~~2.130476415~~ (-3)) 4.615925059(-2)
(033) PRO 2 2.130476415
correct 2.130676415
Relays 6-2 in 033 failed special speed test
In relay " 10,000 test .
Relays changed
1100 Started Cosine Tape (Sine check)
1525 Started Mult + Adder Test.
1545 Relay #70 Panel F
(moth) in relay.
First actual case of bug being found.
1630 arctangent started.
1700 closed down.

Relay
2145
Relay 337

Sources of threats…

Materials

- ***Water*** *– floods, leaks*
- ***Chemicals and particulates -*** *smoke, toxic materials, industrial pollution*
- ***Organism*** *- virus, bacteria, animal, insect*
- *…*

Energy

- ***Fire***
- ***Explosion***
- ***Electricity**, **magnetism, radio wave** anomalies*
- *…*

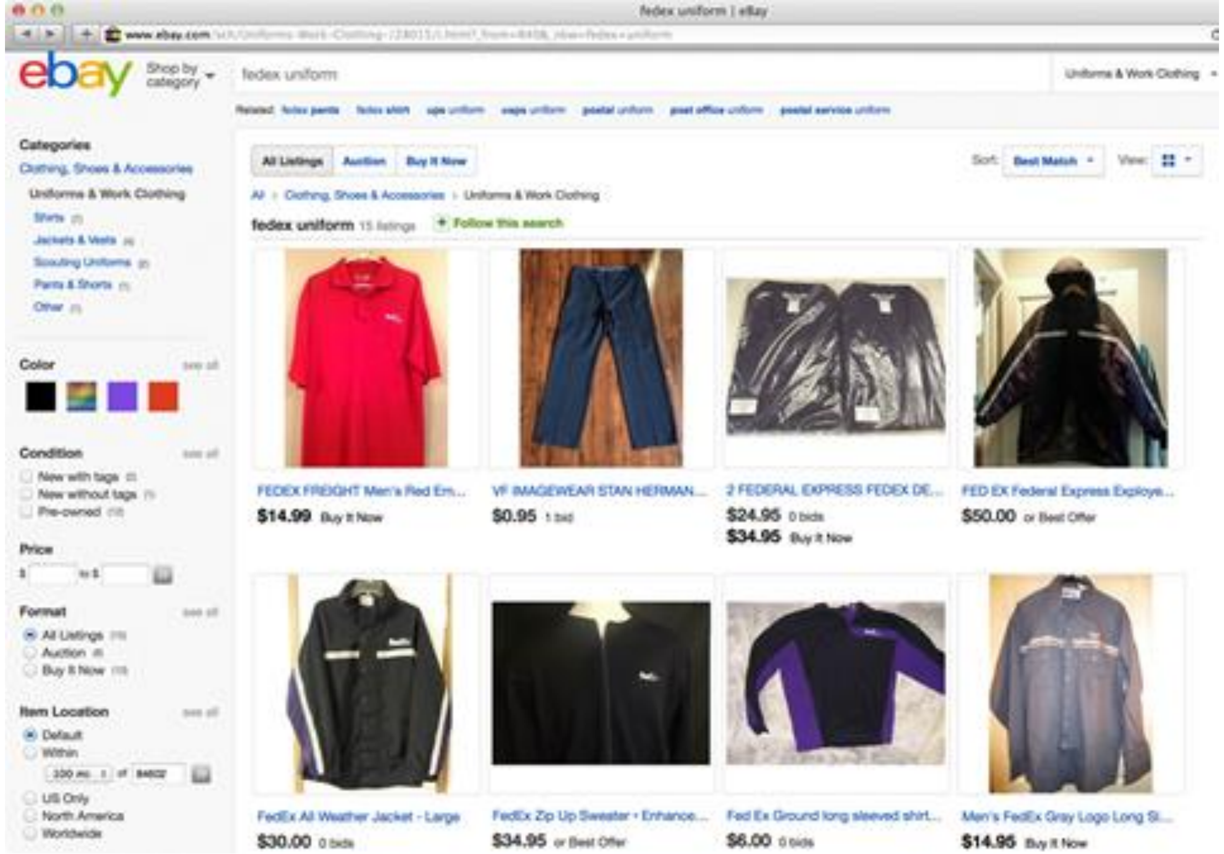
Human *– vandalism, sabotage, theft, terrorism, war*

Human Security Threats: “Tailgating”, “Piggybacking” and Social Engineering

Social engineering

Are receptionists good at preventative security?

- **No,** their job is to help people feel welcome and guide them through the organization in an efficient way
- But intruders can get past guards with social engineering…



FEDEX FREIGHT Men's Red Em...
$14.99 Buy It Now

VF IMAGEWEAR STAN HERMAN...
$0.95 1 bid

2 FEDERAL EXPRESS FEDEX DE...
$24.95 0 bids
$34.95 Buy It Now

FED EX Federal Express Exploye...
$50.00 or Best Offer

FedEx All Weather Jacket - Large
$30.00 0 bids

FedEx Zip Up Sweater + Enhance...
$34.95 or Best Offer

Fed Ex Ground long sleeved shirt...
$6.00 0 bids

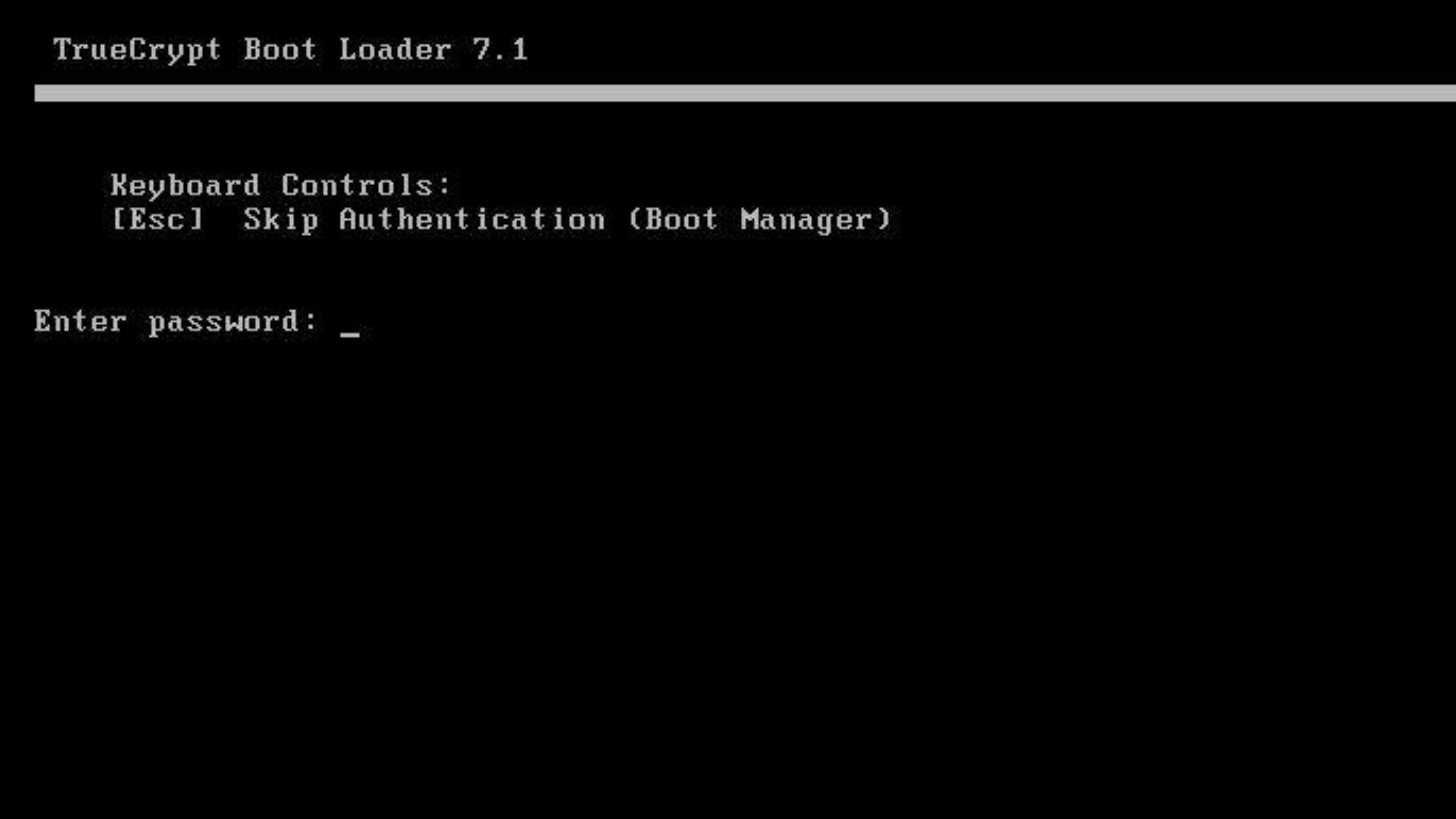
Men's FedEx Gray Logo Long Sl...
$14.95 Buy It Now

NO
HOWARE YOU

What could a hacker do, once in a server room?

Physical access to an unlocked, running system usually means “game over!”

Google | google.com/datacenters

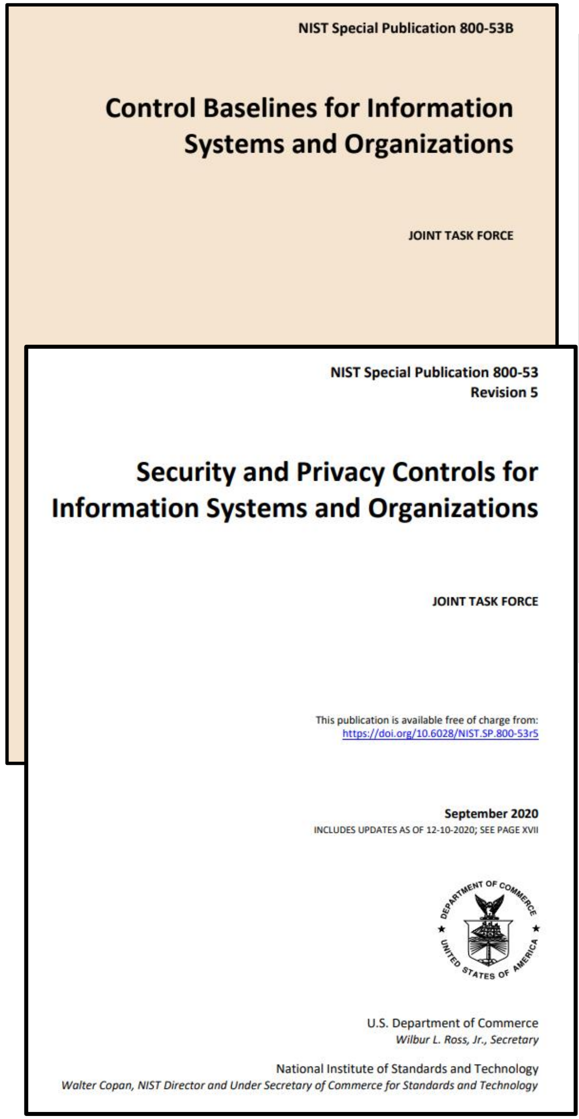


```
 TrueCrypt Boot Loader 7.1


    Keyboard Controls:
    [Esc]  Skip Authentication (Boot Manager)


Enter password: _
```

Cybersecurity controls



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

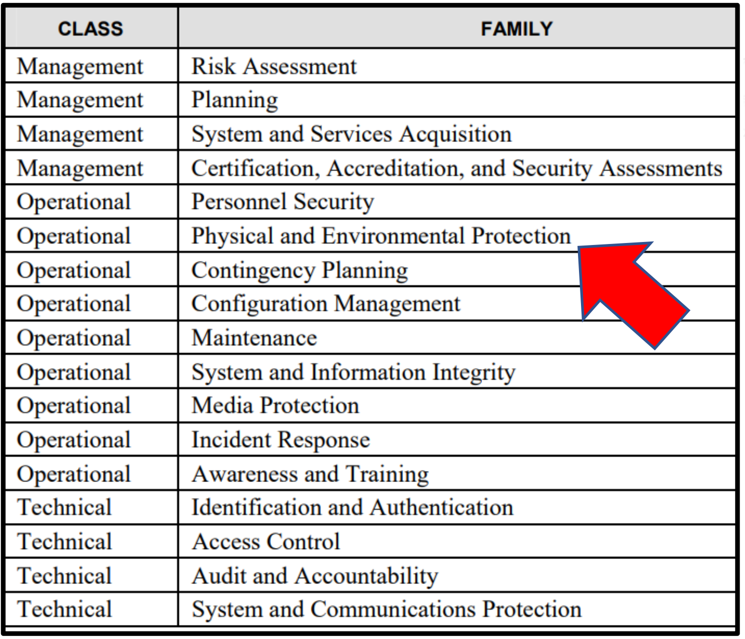
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

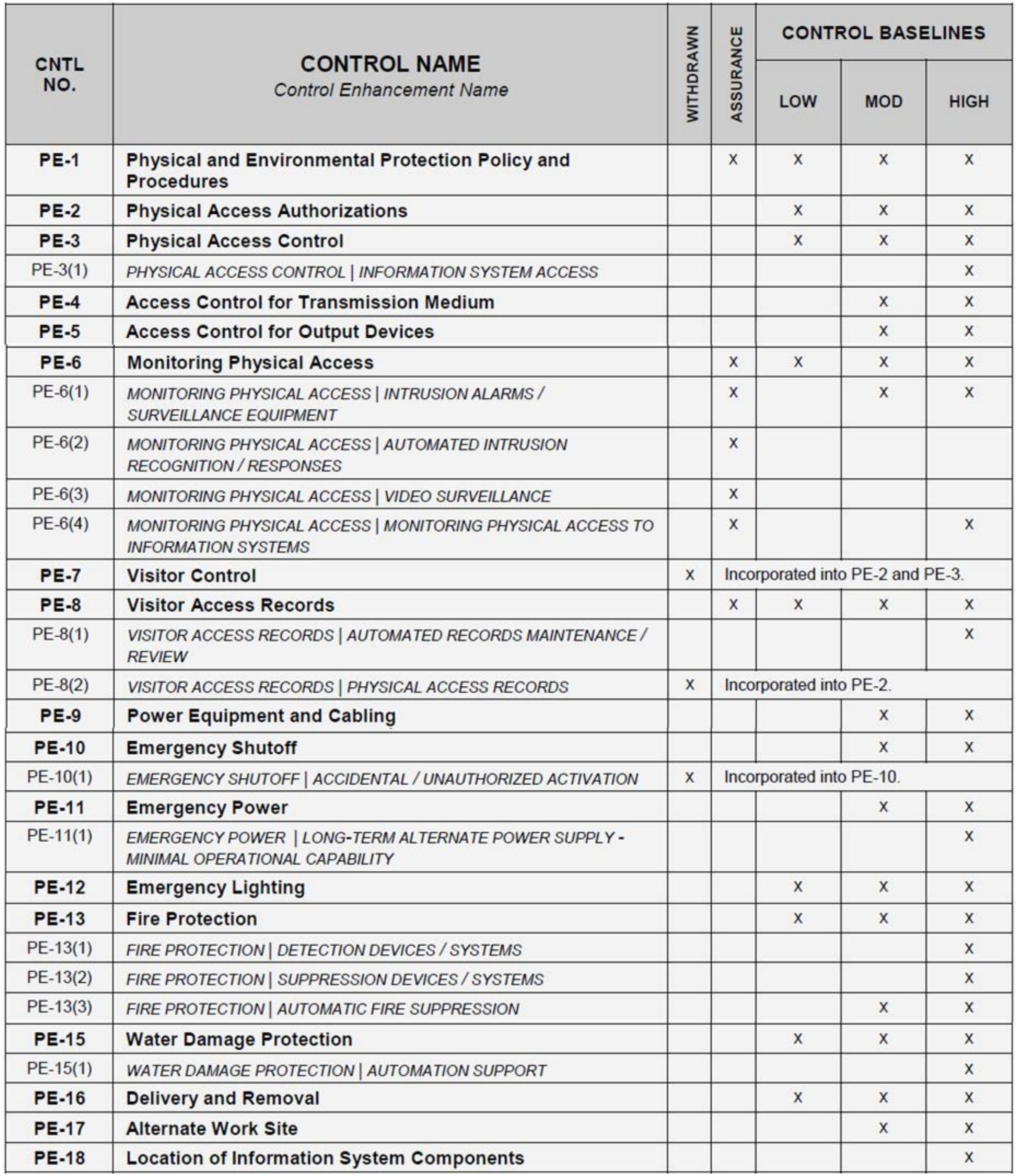
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection



CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
PE-1	**Physical and Environmental Protection Policy and Procedures**		X	X	X	X
PE-2	**Physical Access Authorizations**			X	X	X
PE-3	**Physical Access Control**			X	X	X
PE-3(1)	*PHYSICAL ACCESS CONTROL | INFORMATION SYSTEM ACCESS*					X
PE-4	**Access Control for Transmission Medium**				X	X
PE-5	**Access Control for Output Devices**				X	X
PE-6	**Monitoring Physical Access**		X	X	X	X
PE-6(1)	*MONITORING PHYSICAL ACCESS | INTRUSION ALARMS / SURVEILLANCE EQUIPMENT*		X		X	X
PE-6(2)	*MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION / RESPONSES*		X			
PE-6(3)	*MONITORING PHYSICAL ACCESS | VIDEO SURVEILLANCE*		X			
PE-6(4)	*MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO INFORMATION SYSTEMS*		X			X
PE-7	**Visitor Control**	X	Incorporated into PE-2 and PE-3.			
PE-8	**Visitor Access Records**		X	X	X	X
PE-8(1)	*VISITOR ACCESS RECORDS | AUTOMATED RECORDS MAINTENANCE / REVIEW*					X
PE-8(2)	*VISITOR ACCESS RECORDS | PHYSICAL ACCESS RECORDS*	X	Incorporated into PE-2.			
PE-9	**Power Equipment and Cabling**				X	X
PE-10	**Emergency Shutoff**				X	X
PE-10(1)	*EMERGENCY SHUTOFF | ACCIDENTAL / UNAUTHORIZED ACTIVATION*	X	Incorporated into PE-10.			
PE-11	**Emergency Power**				X	X
PE-11(1)	*EMERGENCY POWER | LONG-TERM ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY*					X
PE-12	**Emergency Lighting**			X	X	X
PE-13	**Fire Protection**			X	X	X
PE-13(1)	*FIRE PROTECTION | DETECTION DEVICES / SYSTEMS*					X
PE-13(2)	*FIRE PROTECTION | SUPPRESSION DEVICES / SYSTEMS*					X
PE-13(3)	*FIRE PROTECTION | AUTOMATIC FIRE SUPPRESSION*				X	X
PE-15	**Water Damage Protection**			X	X	X
PE-15(1)	*WATER DAMAGE PROTECTION | AUTOMATION SUPPORT*					X
PE-16	**Delivery and Removal**			X	X	X
PE-17	**Alternate Work Site**				X	X
PE-18	**Location of Information System Components**					X

Media theft

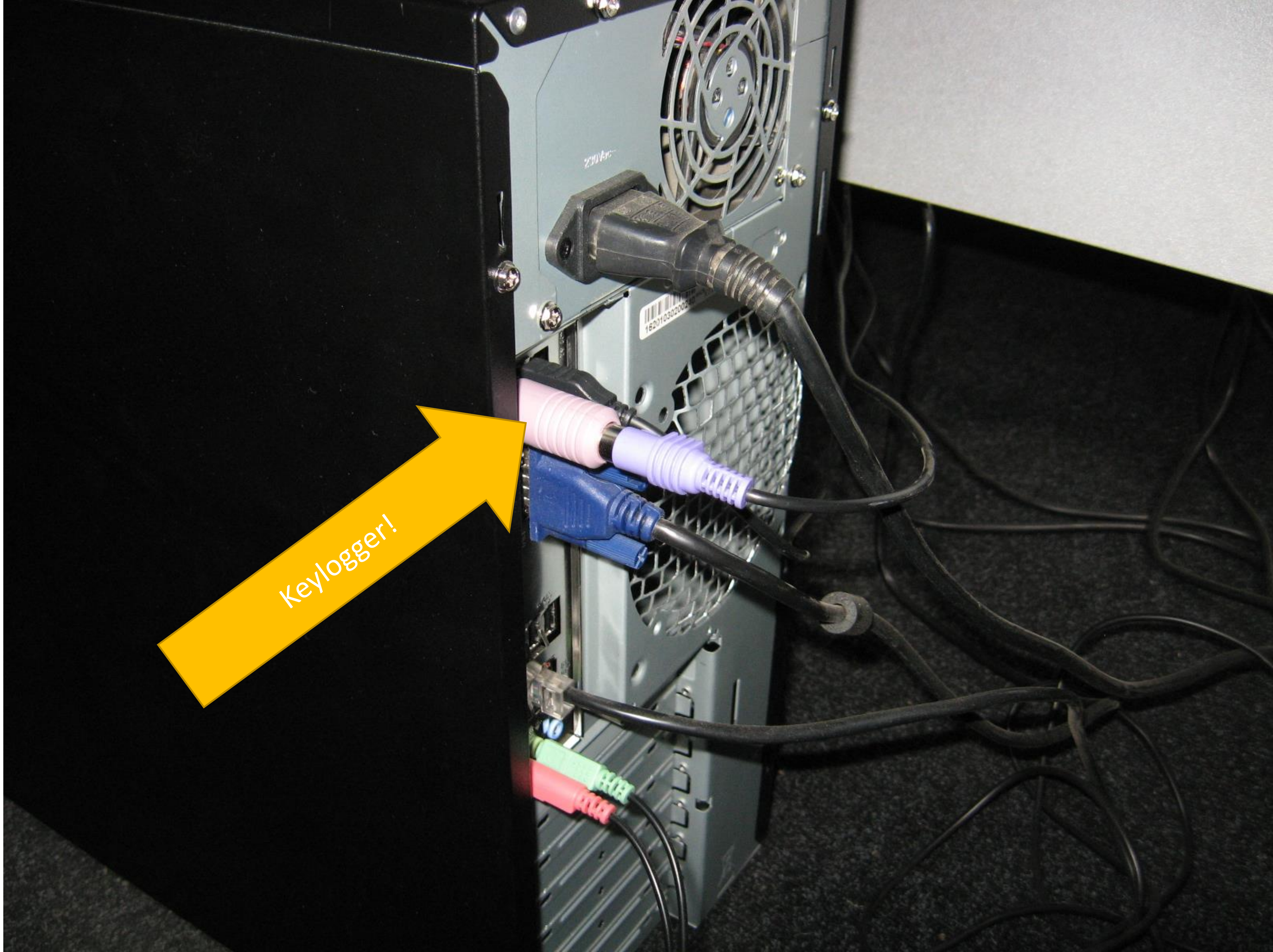
“2020 Cost of a Data Breach Report” by the Ponemon Institute and published by IBM Security

Analyzed 524 breaches that occurred between August 2019 and April 2020, in all sizes of organizations, across 17 industries and 17 geographies

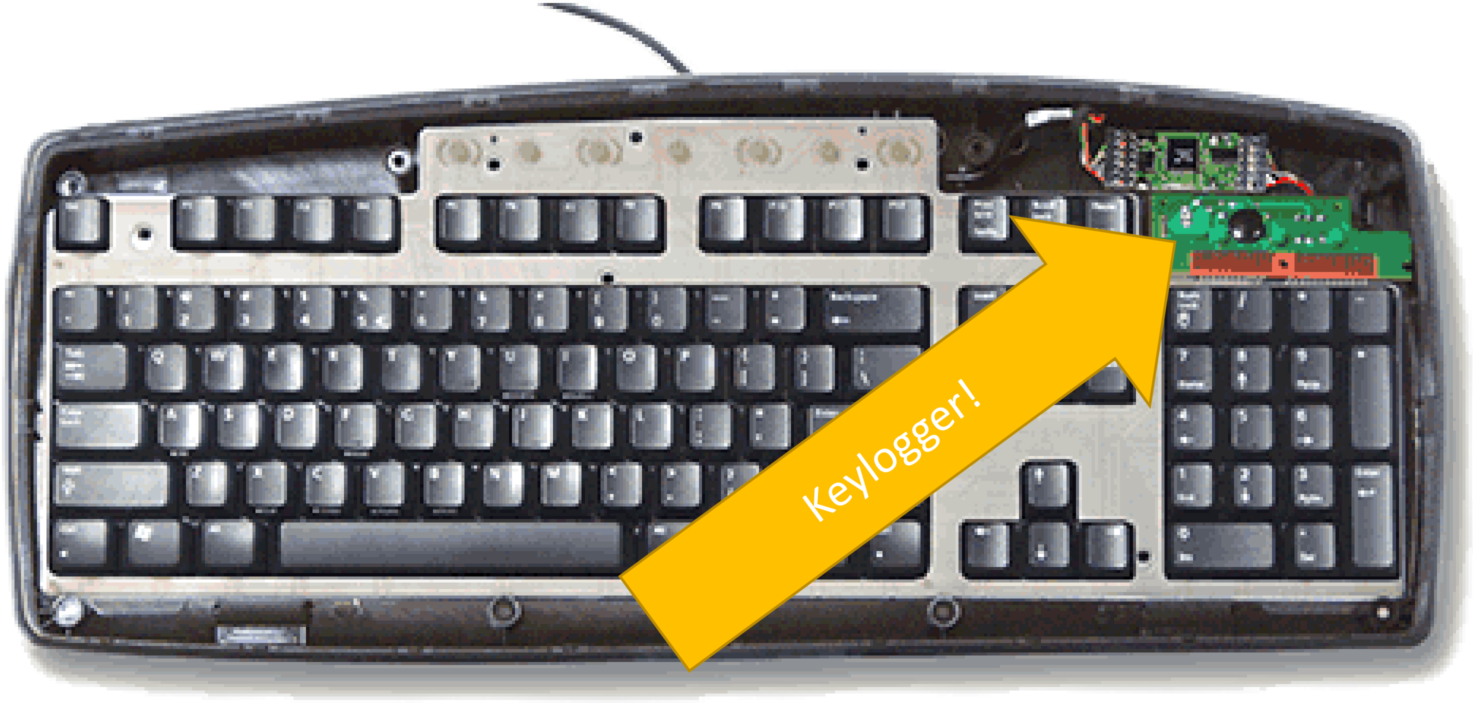
10% of malicious breaches were caused by a physical security compromise, at an average cost of $4.36 million.

Key loggers

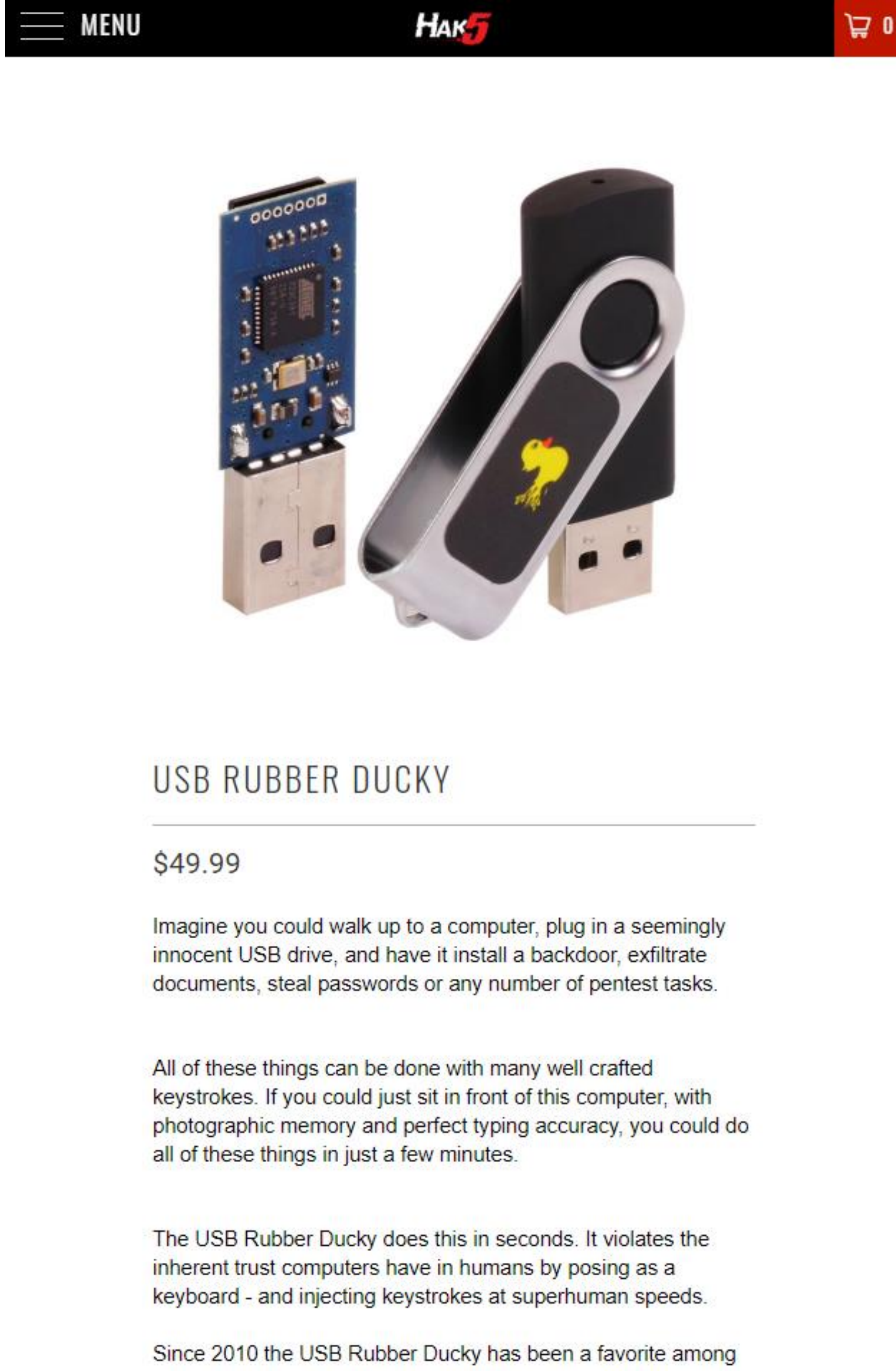
What’s wrong in this photo?



Keyloggers violate federal wiretapping laws



Keystroke injector



USB RUBBER DUCKY

$49.99

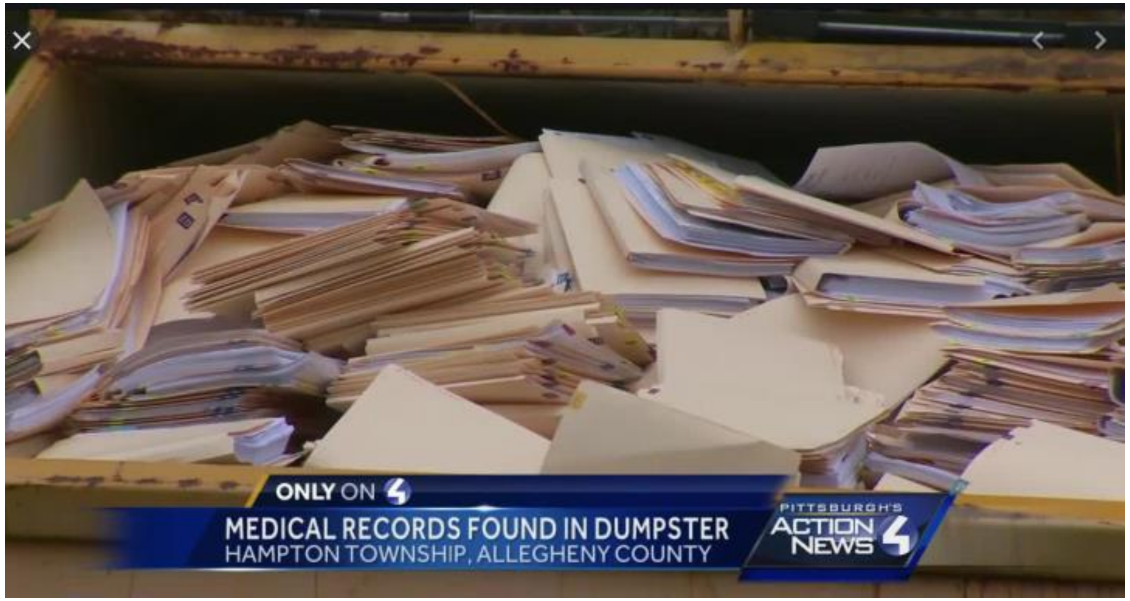
Imagine you could walk up to a computer, plug in a seemingly innocent USB drive, and have it install a backdoor, exfiltrate documents, steal passwords or any number of pentest tasks.

All of these things can be done with many well crafted keystrokes. If you could just sit in front of this computer, with photographic memory and perfect typing accuracy, you could do all of these things in just a few minutes.

The USB Rubber Ducky does this in seconds. It violates the inherent trust computers have in humans by posing as a keyboard - and injecting keystrokes at superhuman speeds.

Since 2010 the USB Rubber Ducky has been a favorite among

“Dumpster diving”


ONLY ON 4
MEDICAL RECORDS FOUND IN DUMPSTER
HAMPTON TOWNSHIP, ALLEGHENY COUNTY
PITTSBURGH'S ACTION NEWS 4

PAPER

Physical Security Control Types

Physical Controls

Perimeter security, fences, lighting, facility construction, keys and locks, access card and readers, …

Administrative Controls

Facility selection, facility construction and management, personnel identity badges and controls, evacuation procedures, system shutdown procedures, fire suppression procedures, hardware failure procedures, bomb threat and lock down procedures,…

Technical Controls

Physical access control and monitoring system, intrusion detection and alarm system, fire detection and suppression system, uninterrupted power supply, heating / ventilation / air conditioning system (HVAC), disk mirroring, data backup,…

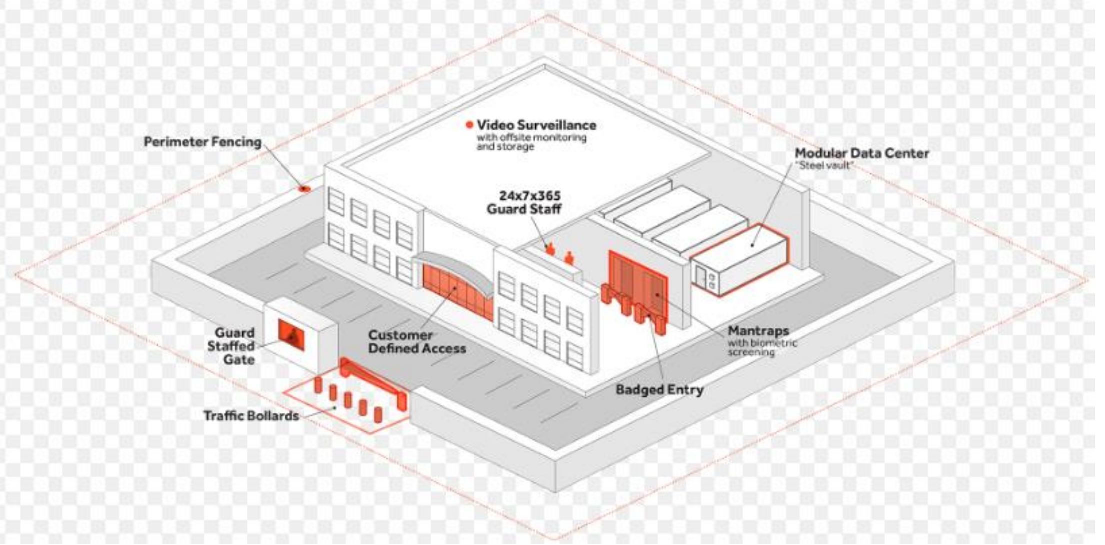
Agenda

- ✓Vulnerabilities and sources of threats
- ✓Physical control inventory baselines
- Perimeter security
- Media protection
- Media sanitization

Perimeter Security

Perimeter security controls are used to prevent, detect and respond to unauthorized access to a facility

Perimeter Control



Fencing – different heights serve different purposes:

- 3 – 4 feet – deter casual trespassers
- 6 – 7 feet – deter general intruders
- 8 feet with barbed wire slanted at a 45^{o} angle – deter more determined intruders

PIDAS – Perimeter Intrusion and Detection Assessment System

- Fencing system with mesh wire and passive cable vibration sensors
- Detects intruder approaching and damaging the fence (may generate many false alarms)

Bollards – Small round concrete pillars placed around a building

- Protects from damage by someone running a vehicle into the side of the building or getting too close for car-bomb

Lighting – Streetlights, floodlights or searchlights

- Good deterrents for unauthorized access and personnel safety
- National Institute of Standards and Technology (NIST) standard requires critical areas to be illuminated 8 feet in height with 2-foot candle power

Target Hardening

Complements natural access controls by using mechanical and/or operational controls:

- alarms, guards and receptionists
- visitor sign-in/sign-out procedures
- picture identification requirements,…

Restricted and work area security often

receive additional physical security controls beyond:

- ***Key card access control systems***
- ***Video surveillance***

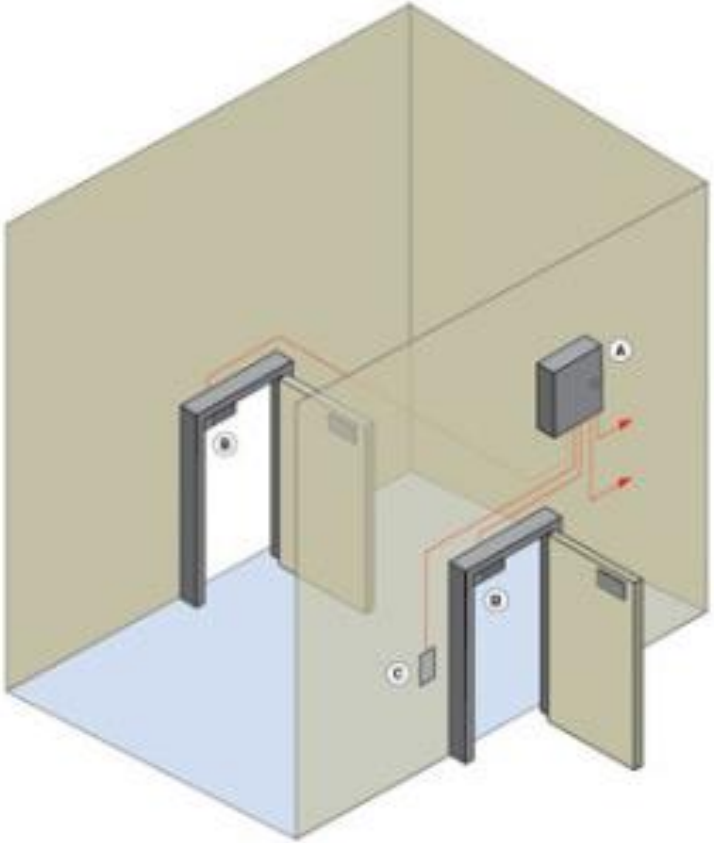
Physical security controls for secure locations may also include:

- **Multi-factor key card entry**
  - Bi-factor (or tri-factor): Key cards + PIN pad or biometric
- **Security guards (and guard dogs)**
  - At ingress/egress points to prevent unauthorized access, roaming facility alert for unauthorized personnel or activities, involved in capture of unauthorized personnel in a facility
- ***Security wall and fences***
  - 1 or more to keep authorized personnel away from facilities
- ***Security cameras and lighting***
  - Additional lighting to expose and deter would-be intruders
- ***Security gates, crash gates, and bollards***
  - Limit the movement of vehicles near a facility to reduce vehicle-borne threats

<u>Physical security controls</u> for secure locations may also include:

Mantrap

- Made of two doors, one for entry, one for exit from the booth/ mantrap
  - When the first door is open, the second remains locked until the first one is closed and the individual inside the booth is cleared by a security operator monitoring this interlocking system

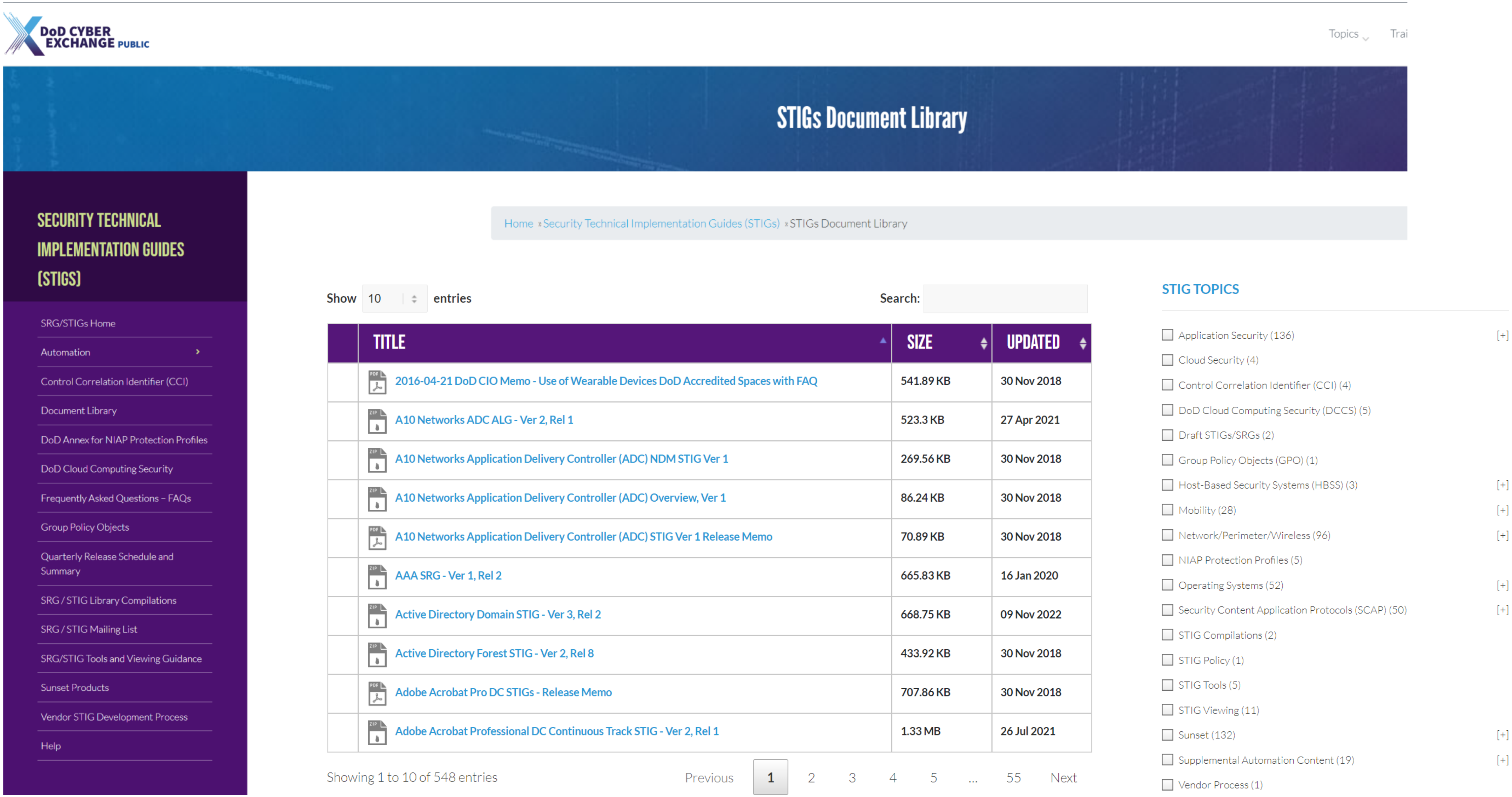


DexID

Agenda

- ✓Vulnerabilities and sources of threats
- ✓Physical control inventory baselines
- ✓Perimeter security
- Media protection
- Media sanitization

Security Technical Implementation Guides



DoD CYBER EXCHANGE PUBLIC

Topics Trai

STIGs Document Library

SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)

- SRG/STIGs Home
- Automation ›
- Control Correlation Identifier (CCI)
- Document Library
- DoD Annex for NIAP Protection Profiles
- DoD Cloud Computing Security
- Frequently Asked Questions – FAQs
- Group Policy Objects
- Quarterly Release Schedule and Summary
- SRG / STIG Library Compilations
- SRG / STIG Mailing List
- SRG/STIG Tools and Viewing Guidance
- Sunset Products
- Vendor STIG Development Process
- Help

Home » Security Technical Implementation Guides (STIGs) » STIGs Document Library

Show 10 entries

Search:

	TITLE	SIZE	UPDATED
	2016-04-21 DoD CIO Memo - Use of Wearable Devices DoD Accredited Spaces with FAQ	541.89 KB	30 Nov 2018
	A10 Networks ADC ALG - Ver 2, Rel 1	523.3 KB	27 Apr 2021
	A10 Networks Application Delivery Controller (ADC) NDM STIG Ver 1	269.56 KB	30 Nov 2018
	A10 Networks Application Delivery Controller (ADC) Overview, Ver 1	86.24 KB	30 Nov 2018
	A10 Networks Application Delivery Controller (ADC) STIG Ver 1 Release Memo	70.89 KB	30 Nov 2018
	AAA SRG - Ver 1, Rel 2	665.83 KB	16 Jan 2020
	Active Directory Domain STIG - Ver 3, Rel 2	668.75 KB	09 Nov 2022
	Active Directory Forest STIG - Ver 2, Rel 8	433.92 KB	30 Nov 2018
	Adobe Acrobat Pro DC STIGs - Release Memo	707.86 KB	30 Nov 2018
	Adobe Acrobat Professional DC Continuous Track STIG - Ver 2, Rel 1	1.33 MB	26 Jul 2021

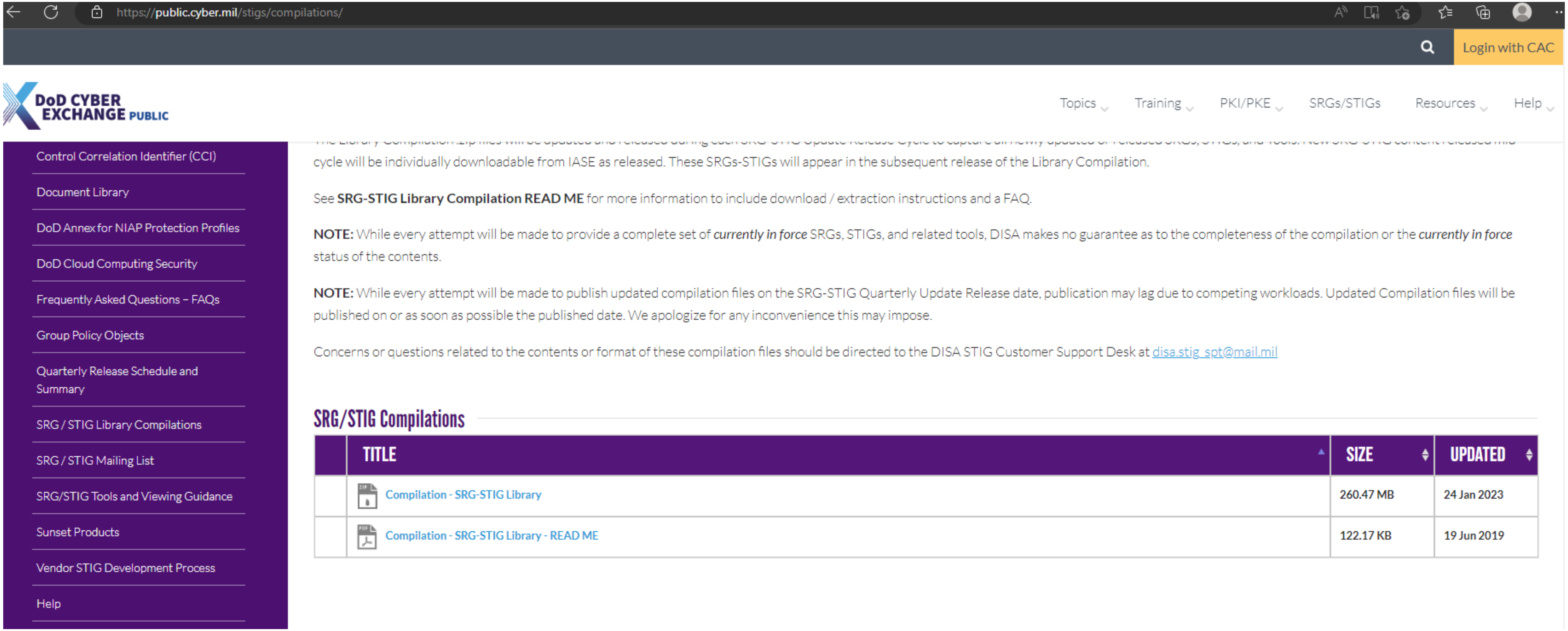
Showing 1 to 10 of 548 entries

Previous 1 2 3 4 5 … 55 Next

STIG TOPICS

- □ Application Security (136) [+]
- □ Cloud Security (4)
- □ Control Correlation Identifier (CCI) (4)
- □ DoD Cloud Computing Security (DCCS) (5)
- □ Draft STIGs/SRGs (2)
- □ Group Policy Objects (GPO) (1)
- □ Host-Based Security Systems (HBSS) (3) [+]
- □ Mobility (28) [+]
- □ Network/Perimeter/Wireless (96) [+]
- □ NIAP Protection Profiles (5)
- □ Operating Systems (52) [+]
- □ Security Content Application Protocols (SCAP) (50) [+]
- □ STIG Compilations (2)
- □ STIG Policy (1)
- □ STIG Tools (5)
- □ STIG Viewing (11)
- □ Sunset (132) [+]
- □ Supplemental Automation Content (19) [+]
- □ Vendor Process (1)

Security Requirements Guides (SRGs) and Security Technical Implemtation Guides (STIGs)


https://public.cyber.mil/stigs/compilations/
Login with CAC
DoD CYBER EXCHANGE PUBLIC
Topics
Training
PKI/PKE
SRGs/STIGs
Resources
Help
Control Correlation Identifier (CCI)
Document Library
DoD Annex for NIAP Protection Profiles
DoD Cloud Computing Security
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
Vendor STIG Development Process
Help

The Library Compilation .zip files will be updated and released during each SRG-STIG Update Release Cycle to capture all newly updated or released SRGs, STIGs, and Tools. New SRG-STIG content released mid-cycle will be individually downloadable from IASE as released. These SRGs-STIGs will appear in the subsequent release of the Library Compilation.

See **SRG-STIG Library Compilation READ ME** for more information to include download / extraction instructions and a FAQ.

NOTE: While every attempt will be made to provide a complete set of ***currently in force*** SRGs, STIGs, and related tools, DISA makes no guarantee as to the completeness of the compilation or the ***currently in force*** status of the contents.

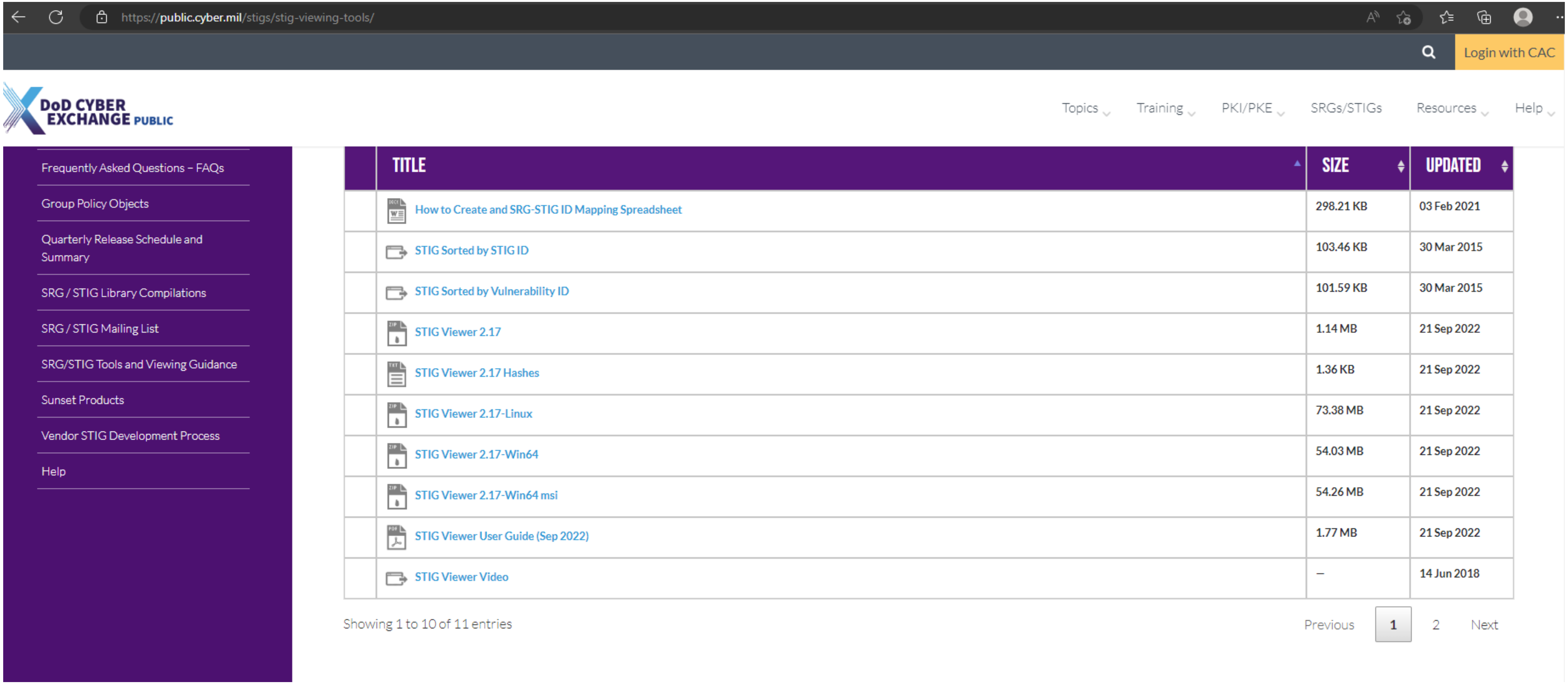
NOTE: While every attempt will be made to publish updated compilation files on the SRG-STIG Quarterly Update Release date, publication may lag due to competing workloads. Updated Compilation files will be published on or as soon as possible the published date. We apologize for any inconvenience this may impose.

Concerns or questions related to the contents or format of these compilation files should be directed to the DISA STIG Customer Support Desk at disa.stig_spt@mail.mil

SRG/STIG Compilations

	TITLE	SIZE	UPDATED
	Compilation - SRG-STIG Library	260.47 MB	24 Jan 2023
	Compilation - SRG-STIG Library - READ ME	122.17 KB	19 Jun 2019

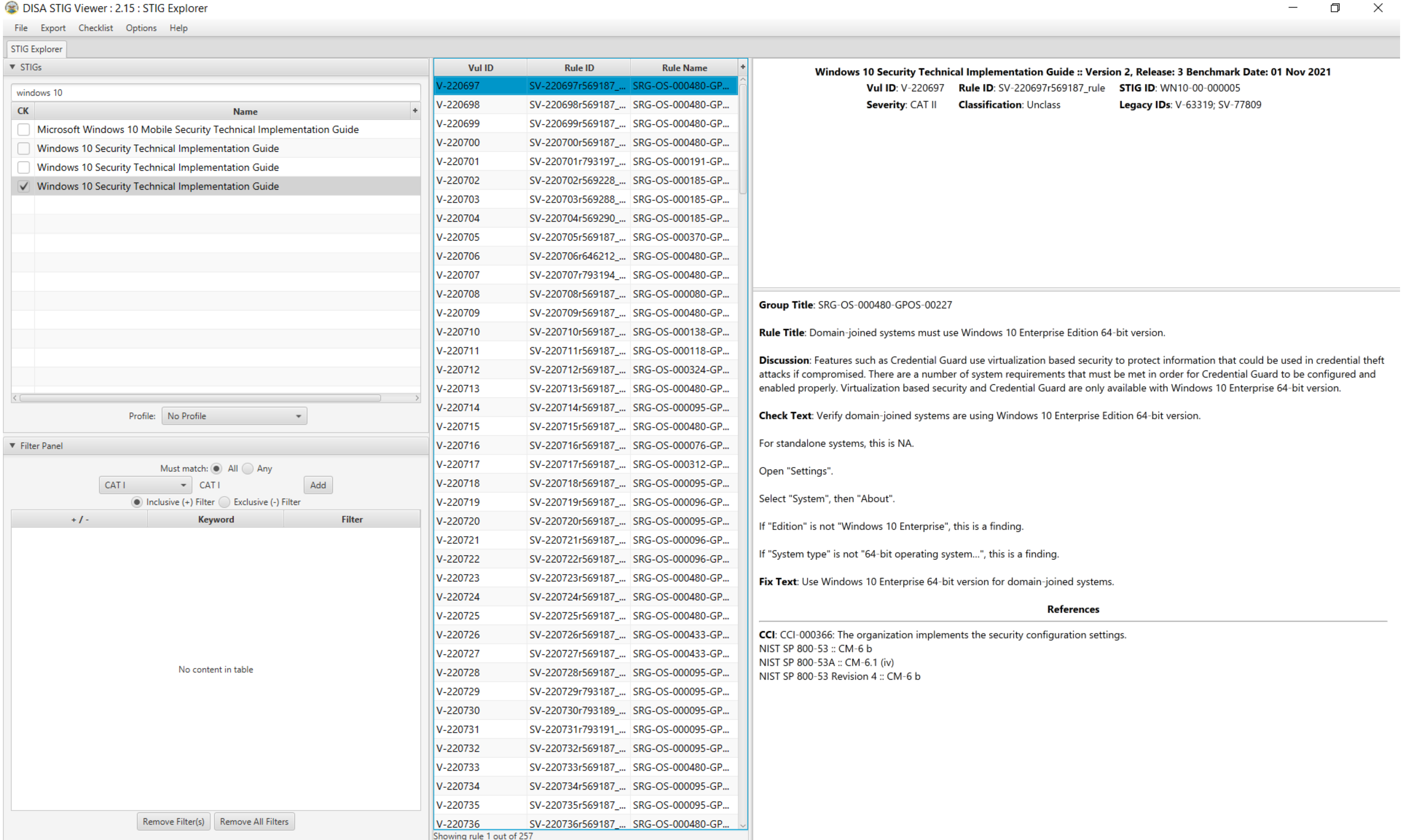
STIG Viewer



https://public.cyber.mil/stigs/stig-viewing-tools/
Login with CAC
DoD CYBER EXCHANGE PUBLIC
Topics
Training
PKI/PKE
SRGs/STIGs
Resources
Help
Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
Vendor STIG Development Process
Help

TITLE	SIZE	UPDATED
How to Create and SRG-STIG ID Mapping Spreadsheet	298.21 KB	03 Feb 2021
STIG Sorted by STIG ID	103.46 KB	30 Mar 2015
STIG Sorted by Vulnerability ID	101.59 KB	30 Mar 2015
STIG Viewer 2.17	1.14 MB	21 Sep 2022
STIG Viewer 2.17 Hashes	1.36 KB	21 Sep 2022
STIG Viewer 2.17-Linux	73.38 MB	21 Sep 2022
STIG Viewer 2.17-Win64	54.03 MB	21 Sep 2022
STIG Viewer 2.17-Win64 msi	54.26 MB	21 Sep 2022
STIG Viewer User Guide (Sep 2022)	1.77 MB	21 Sep 2022
STIG Viewer Video	–	14 Jun 2018

Showing 1 to 10 of 11 entries



windows 10

CK	Name
☐	Microsoft Windows 10 Mobile Security Technical Implementation Guide
☐	Windows 10 Security Technical Implementation Guide
☐	Windows 10 Security Technical Implementation Guide
☑	Windows 10 Security Technical Implementation Guide

Profile: No Profile

Must match: ● All ○ Any

CAT I CAT I

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

Vul ID	Rule ID	Rule Name
V-220697	SV-220697r569187_...	SRG-OS-000480-GP...
V-220698	SV-220698r569187_...	SRG-OS-000480-GP...
V-220699	SV-220699r569187_...	SRG-OS-000480-GP...
V-220700	SV-220700r569187_...	SRG-OS-000480-GP...
V-220701	SV-220701r793197_...	SRG-OS-000191-GP...
V-220702	SV-220702r569228_...	SRG-OS-000185-GP...
V-220703	SV-220703r569288_...	SRG-OS-000185-GP...
V-220704	SV-220704r569290_...	SRG-OS-000185-GP...
V-220705	SV-220705r569187_...	SRG-OS-000370-GP...
V-220706	SV-220706r646212_...	SRG-OS-000480-GP...
V-220707	SV-220707r793194_...	SRG-OS-000480-GP...
V-220708	SV-220708r569187_...	SRG-OS-000080-GP...
V-220709	SV-220709r569187_...	SRG-OS-000480-GP...
V-220710	SV-220710r569187_...	SRG-OS-000138-GP...
V-220711	SV-220711r569187_...	SRG-OS-000118-GP...
V-220712	SV-220712r569187_...	SRG-OS-000324-GP...
V-220713	SV-220713r569187_...	SRG-OS-000480-GP...
V-220714	SV-220714r569187_...	SRG-OS-000095-GP...
V-220715	SV-220715r569187_...	SRG-OS-000480-GP...
V-220716	SV-220716r569187_...	SRG-OS-000076-GP...
V-220717	SV-220717r569187_...	SRG-OS-000312-GP...
V-220718	SV-220718r569187_...	SRG-OS-000095-GP...
V-220719	SV-220719r569187_...	SRG-OS-000096-GP...
V-220720	SV-220720r569187_...	SRG-OS-000095-GP...
V-220721	SV-220721r569187_...	SRG-OS-000096-GP...
V-220722	SV-220722r569187_...	SRG-OS-000096-GP...
V-220723	SV-220723r569187_...	SRG-OS-000480-GP...
V-220724	SV-220724r569187_...	SRG-OS-000480-GP...
V-220725	SV-220725r569187_...	SRG-OS-000480-GP...
V-220726	SV-220726r569187_...	SRG-OS-000433-GP...
V-220727	SV-220727r569187_...	SRG-OS-000433-GP...
V-220728	SV-220728r569187_...	SRG-OS-000095-GP...
V-220729	SV-220729r793187_...	SRG-OS-000095-GP...
V-220730	SV-220730r793189_...	SRG-OS-000095-GP...
V-220731	SV-220731r793191_...	SRG-OS-000095-GP...
V-220732	SV-220732r569187_...	SRG-OS-000095-GP...
V-220733	SV-220733r569187_...	SRG-OS-000480-GP...
V-220734	SV-220734r569187_...	SRG-OS-000095-GP...
V-220735	SV-220735r569187_...	SRG-OS-000095-GP...
V-220736	SV-220736r569187_...	SRG-OS-000480-GP...

Showing rule 1 out of 257

Windows 10 Security Technical Implementation Guide :: Version 2, Release: 3 Benchmark Date: 01 Nov 2021

Vul ID: V-220697 **Rule ID**: SV-220697r569187_rule **STIG ID**: WN10-00-000005

Severity: CAT II **Classification**: Unclass **Legacy IDs**: V-63319; SV-77809

Group Title: SRG-OS-000480-GPOS-00227

Rule Title: Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.

Discussion: Features such as Credential Guard use virtualization based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise 64-bit version.

Check Text: Verify domain-joined systems are using Windows 10 Enterprise Edition 64-bit version.

For standalone systems, this is NA.

Open "Settings".

Select "System", then "About".

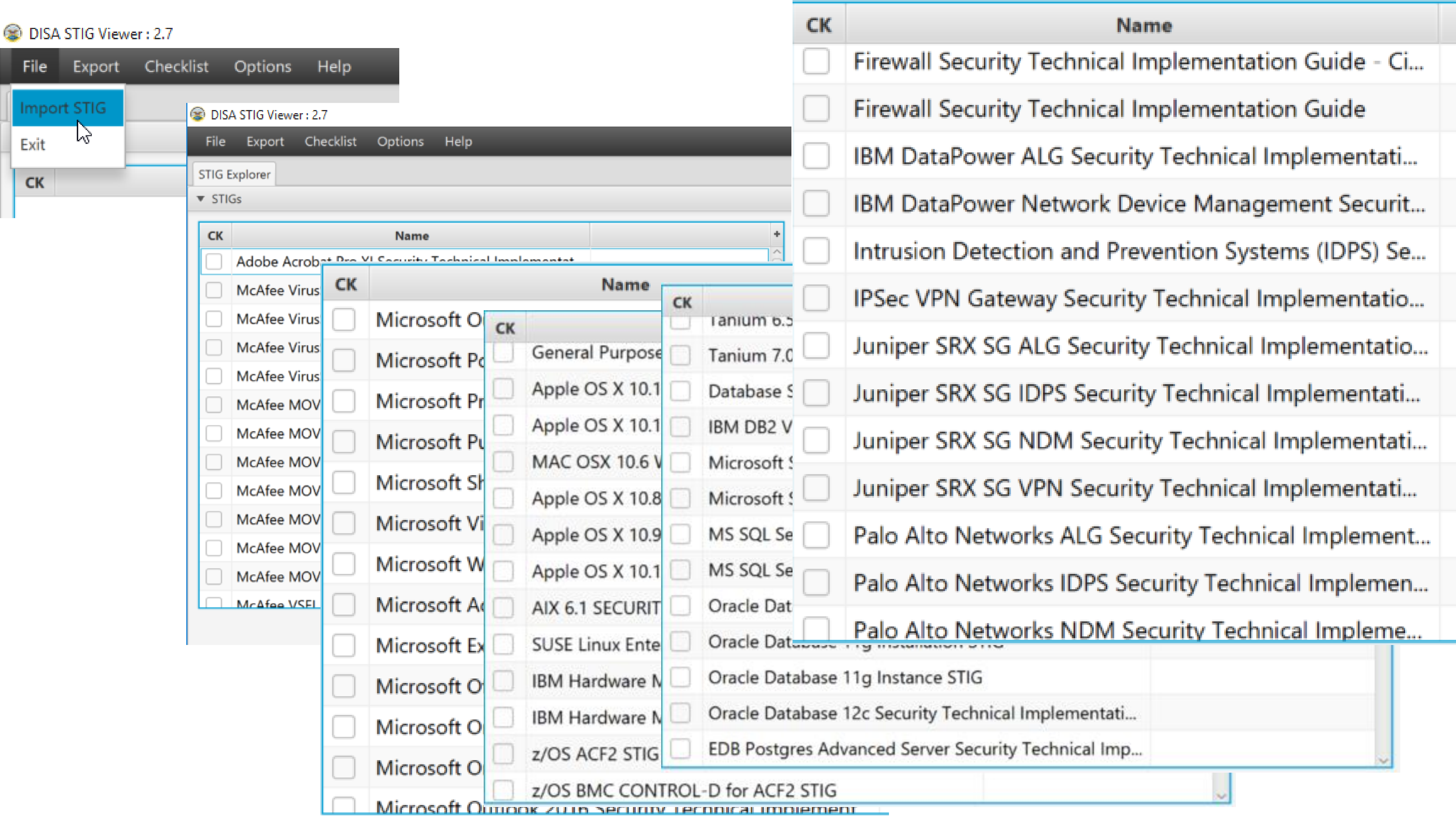
If "Edition" is not "Windows 10 Enterprise", this is a finding.

If "System type" is not "64-bit operating system...", this is a finding.

Fix Text: Use Windows 10 Enterprise 64-bit version for domain-joined systems.

References

CCI: CCI-000366: The organization implements the security configuration settings.
NIST SP 800-53 :: CM-6 b
NIST SP 800-53A :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b



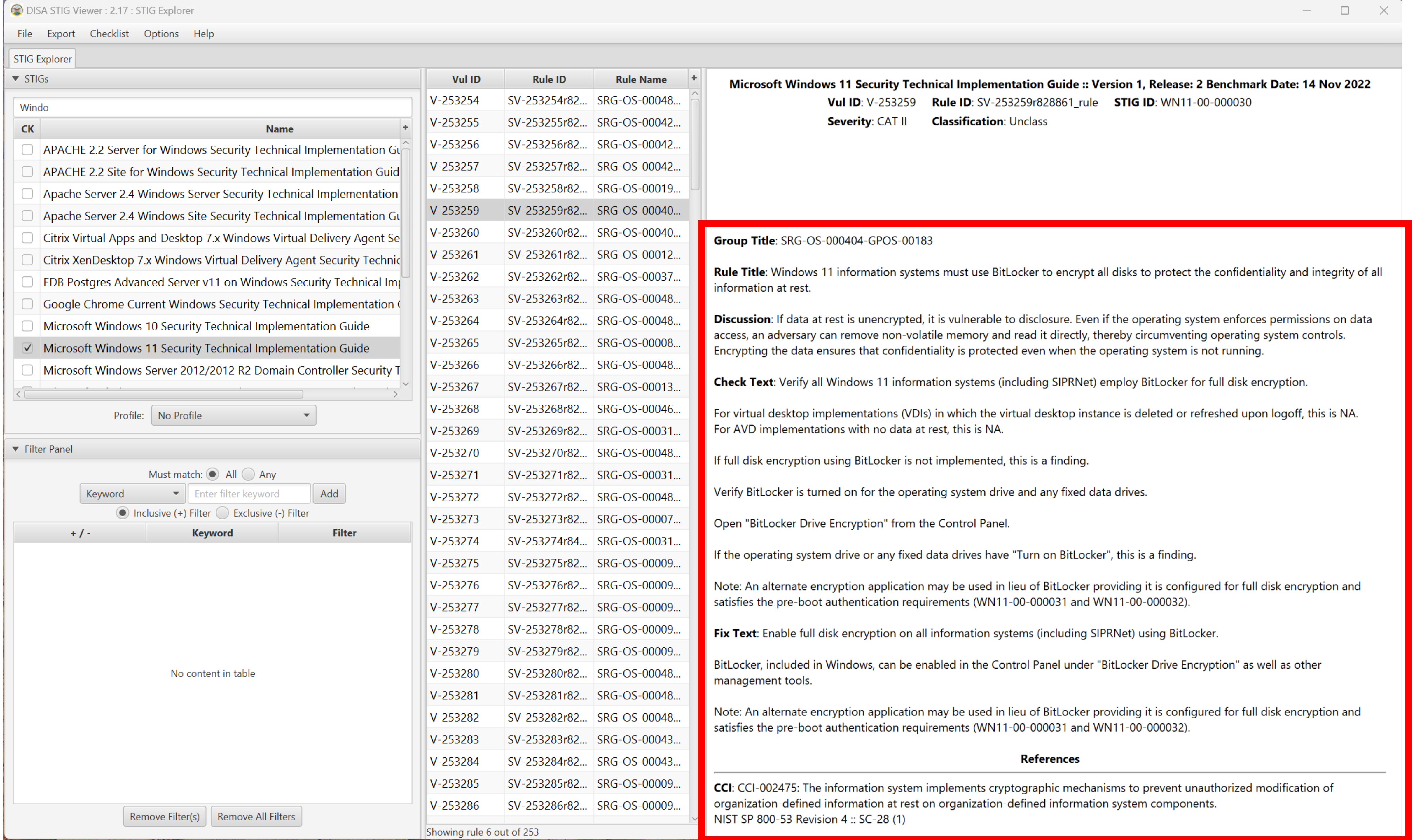
CK	Name
□	Adobe Acrobat Pro XI Security Technical Implementat...
□	McAfee Virus
□	McAfee Virus
□	McAfee Virus
□	McAfee Virus
□	McAfee MOV
□	McAfee MOV
□	McAfee MOV
□	McAfee MOV
□	McAfee MOV
□	McAfee MOV
□	McAfee MOV
□	McAfee VSEL

CK	Name
□	Microsoft O
□	Microsoft Po
□	Microsoft Pr
□	Microsoft Pu
□	Microsoft Sh
□	Microsoft Vi
□	Microsoft W
□	Microsoft Ac
□	Microsoft Ex
□	Microsoft O
□	Microsoft O
□	Microsoft O
□	Microsoft Outlook 2016 Security Technical Implement

CK	Name
□	General Purpose
□	Apple OS X 10.1
□	Apple OS X 10.1
□	MAC OSX 10.6 V
□	Apple OS X 10.8
□	Apple OS X 10.9
□	Apple OS X 10.1
□	AIX 6.1 SECURIT
□	SUSE Linux Ente
□	IBM Hardware M
□	IBM Hardware M
□	z/OS ACF2 STIG
□	z/OS BMC CONTROL-D for ACF2 STIG

CK	Name
□	Tanium 6.5
□	Tanium 7.0
□	Database S
□	IBM DB2 V
□	Microsoft S
□	Microsoft S
□	MS SQL Se
□	MS SQL Se
□	Oracle Dat
□	Oracle Database 11g Installation STIG
□	Oracle Database 11g Instance STIG
□	Oracle Database 12c Security Technical Implementati...
□	EDB Postgres Advanced Server Security Technical Imp...

CK	Name
□	Firewall Security Technical Implementation Guide - Ci...
□	Firewall Security Technical Implementation Guide
□	IBM DataPower ALG Security Technical Implementati...
□	IBM DataPower Network Device Management Securit...
□	Intrusion Detection and Prevention Systems (IDPS) Se...
□	IPSec VPN Gateway Security Technical Implementatio...
□	Juniper SRX SG ALG Security Technical Implementatio...
□	Juniper SRX SG IDPS Security Technical Implementati...
□	Juniper SRX SG NDM Security Technical Implementati...
□	Juniper SRX SG VPN Security Technical Implementati...
□	Palo Alto Networks ALG Security Technical Implement...
□	Palo Alto Networks IDPS Security Technical Implemen...
□	Palo Alto Networks NDM Security Technical Impleme...



Windo

CK	Name
□	APACHE 2.2 Server for Windows Security Technical Implementation Gu
□	APACHE 2.2 Site for Windows Security Technical Implementation Guid
□	Apache Server 2.4 Windows Server Security Technical Implementation
□	Apache Server 2.4 Windows Site Security Technical Implementation Gu
□	Citrix Virtual Apps and Desktop 7.x Windows Virtual Delivery Agent Se
□	Citrix XenDesktop 7.x Windows Virtual Delivery Agent Security Technic
□	EDB Postgres Advanced Server v11 on Windows Security Technical Im
□	Google Chrome Current Windows Security Technical Implementation (
□	Microsoft Windows 10 Security Technical Implementation Guide
☑	Microsoft Windows 11 Security Technical Implementation Guide
□	Microsoft Windows Server 2012/2012 R2 Domain Controller Security T

Profile: No Profile

Must match: ● All ○ Any

Keyword | Enter filter keyword | Add

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

Vul ID	Rule ID	Rule Name
V-253254	SV-253254r82...	SRG-OS-00048...
V-253255	SV-253255r82...	SRG-OS-00042...
V-253256	SV-253256r82...	SRG-OS-00042...
V-253257	SV-253257r82...	SRG-OS-00042...
V-253258	SV-253258r82...	SRG-OS-00019...
V-253259	SV-253259r82...	SRG-OS-00040...
V-253260	SV-253260r82...	SRG-OS-00040...
V-253261	SV-253261r82...	SRG-OS-00012...
V-253262	SV-253262r82...	SRG-OS-00037...
V-253263	SV-253263r82...	SRG-OS-00048...
V-253264	SV-253264r82...	SRG-OS-00048...
V-253265	SV-253265r82...	SRG-OS-00008...
V-253266	SV-253266r82...	SRG-OS-00048...
V-253267	SV-253267r82...	SRG-OS-00013...
V-253268	SV-253268r82...	SRG-OS-00046...
V-253269	SV-253269r82...	SRG-OS-00031...
V-253270	SV-253270r82...	SRG-OS-00048...
V-253271	SV-253271r82...	SRG-OS-00031...
V-253272	SV-253272r82...	SRG-OS-00048...
V-253273	SV-253273r82...	SRG-OS-00007...
V-253274	SV-253274r84...	SRG-OS-00031...
V-253275	SV-253275r82...	SRG-OS-00009...
V-253276	SV-253276r82...	SRG-OS-00009...
V-253277	SV-253277r82...	SRG-OS-00009...
V-253278	SV-253278r82...	SRG-OS-00009...
V-253279	SV-253279r82...	SRG-OS-00009...
V-253280	SV-253280r82...	SRG-OS-00048...
V-253281	SV-253281r82...	SRG-OS-00048...
V-253282	SV-253282r82...	SRG-OS-00048...
V-253283	SV-253283r82...	SRG-OS-00043...
V-253284	SV-253284r82...	SRG-OS-00043...
V-253285	SV-253285r82...	SRG-OS-00009...
V-253286	SV-253286r82...	SRG-OS-00009...

Showing rule 6 out of 253

Microsoft Windows 11 Security Technical Implementation Guide :: Version 1, Release: 2 Benchmark Date: 14 Nov 2022

Vul ID: V-253259 **Rule ID**: SV-253259r828861_rule **STIG ID**: WN11-00-000030

Severity: CAT II **Classification**: Unclass

Group Title: SRG-OS-000404-GPOS-00183

Rule Title: Windows 11 information systems must use BitLocker to encrypt all disks to protect the confidentiality and integrity of all information at rest.

Discussion: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running.

Check Text: Verify all Windows 11 information systems (including SIPRNet) employ BitLocker for full disk encryption.

For virtual desktop implementations (VDIs) in which the virtual desktop instance is deleted or refreshed upon logoff, this is NA.
For AVD implementations with no data at rest, this is NA.

If full disk encryption using BitLocker is not implemented, this is a finding.

Verify BitLocker is turned on for the operating system drive and any fixed data drives.

Open "BitLocker Drive Encryption" from the Control Panel.

If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.

Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032).

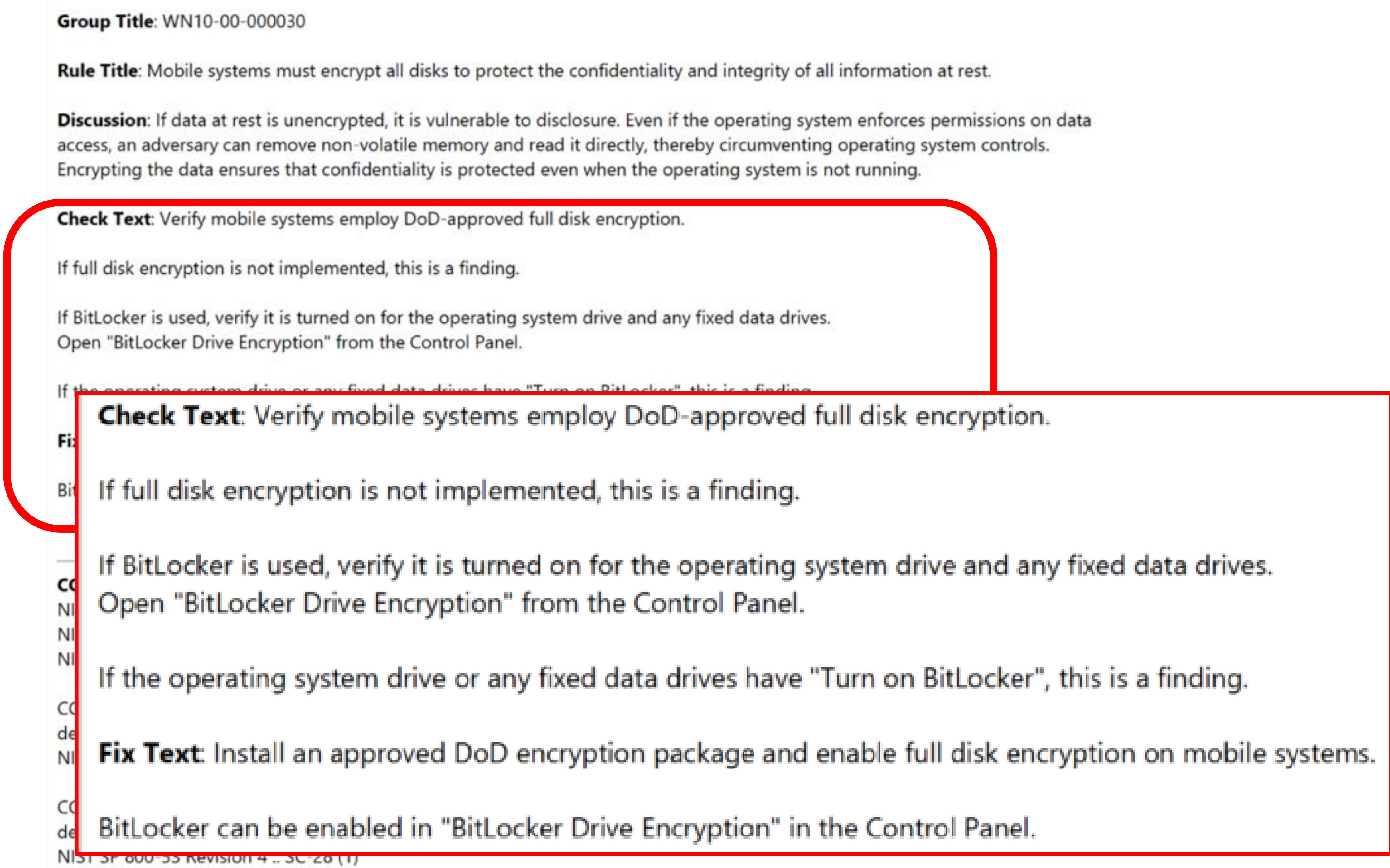
Fix Text: Enable full disk encryption on all information systems (including SIPRNet) using BitLocker.

BitLocker, included in Windows, can be enabled in the Control Panel under "BitLocker Drive Encryption" as well as other management tools.

Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032).

References

CCI: CCI-002475: The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.
NIST SP 800-53 Revision 4 :: SC-28 (1)



Group Title: WN10-00-000030

Rule Title: Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.

Discussion: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running.

Check Text: Verify mobile systems employ DoD-approved full disk encryption.

If full disk encryption is not implemented, this is a finding.

If BitLocker is used, verify it is turned on for the operating system drive and any fixed data drives.
Open "BitLocker Drive Encryption" from the Control Panel.

Check Text: Verify mobile systems employ DoD-approved full disk encryption.

If full disk encryption is not implemented, this is a finding.

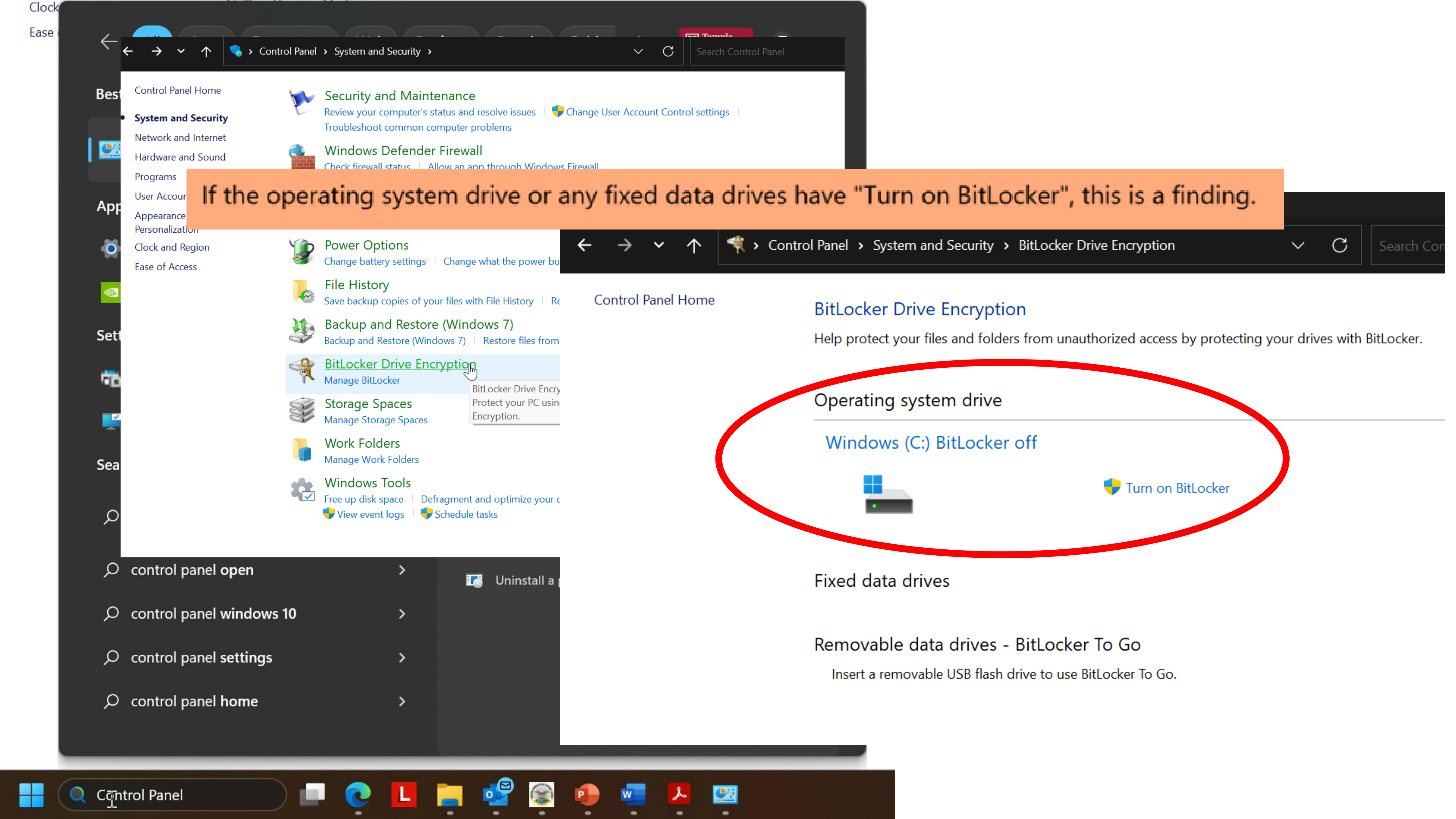
If BitLocker is used, verify it is turned on for the operating system drive and any fixed data drives.
Open "BitLocker Drive Encryption" from the Control Panel.

If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.

Fix Text: Install an approved DoD encryption package and enable full disk encryption on mobile systems.

BitLocker can be enabled in "BitLocker Drive Encryption" in the Control Panel.

NIST SP 800-53 Revision 4 :: SC-28 (1)



If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.

Control Panel › System and Security ›

Control Panel Home

System and Security

Network and Internet

Hardware and Sound

Programs

User Accour

Appearance
Personalization

Clock and Region

Ease of Access

Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems

Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall

Power Options
Change battery settings | Change what the power bu

File History
Save backup copies of your files with File History | Re

Backup and Restore (Windows 7)
Backup and Restore (Windows 7) | Restore files from

BitLocker Drive Encryption
Manage BitLocker

BitLocker Drive Encry
Protect your PC usin
Encryption.

Storage Spaces
Manage Storage Spaces

Work Folders
Manage Work Folders

Windows Tools
Free up disk space | Defragment and optimize your c
View event logs | Schedule tasks

control panel open

control panel windows 10

control panel settings

control panel home

Uninstall a

Control Panel › System and Security › BitLocker Drive Encryption

Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

Windows (C:) BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

Media protection

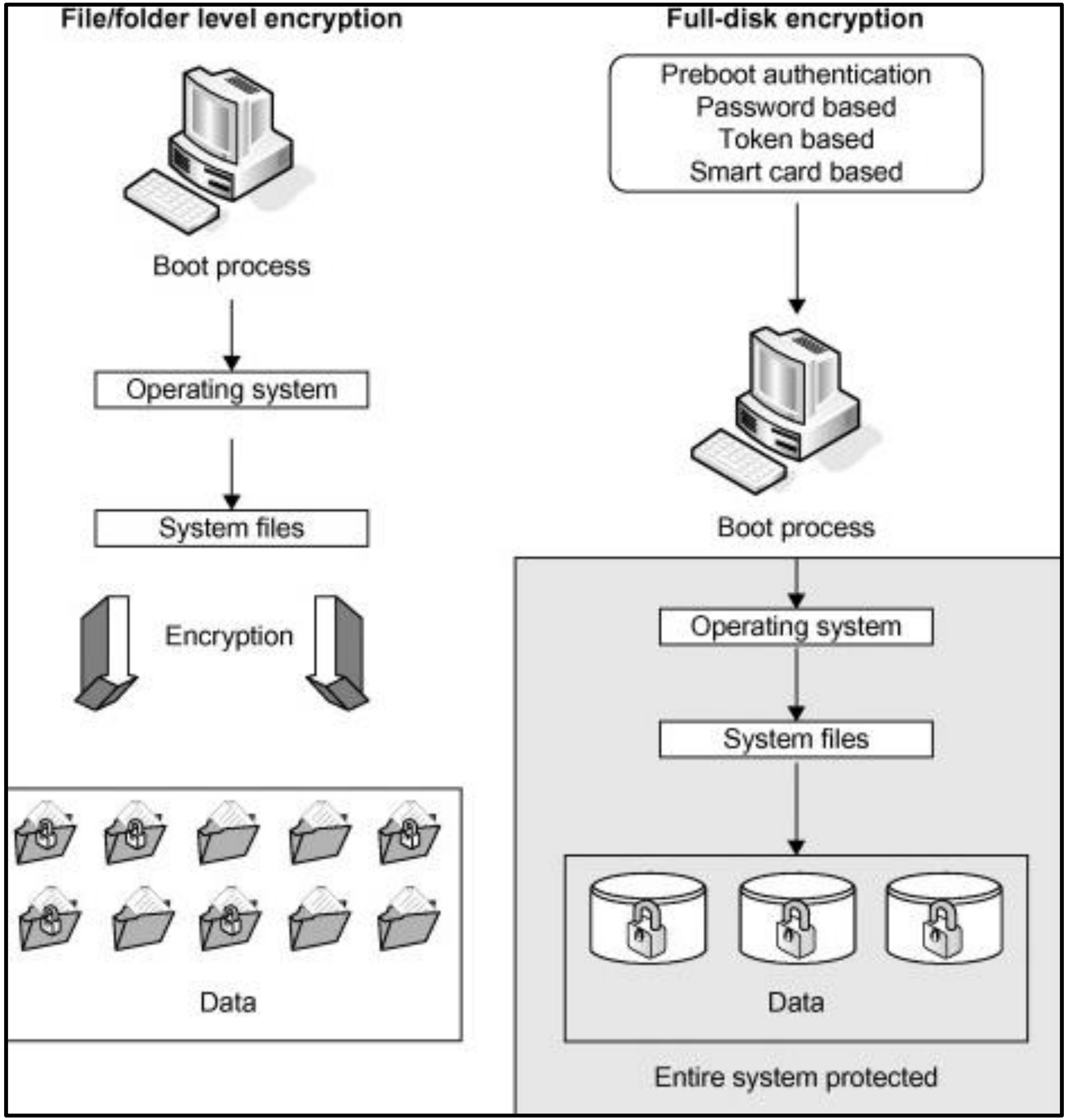
Bitlocker

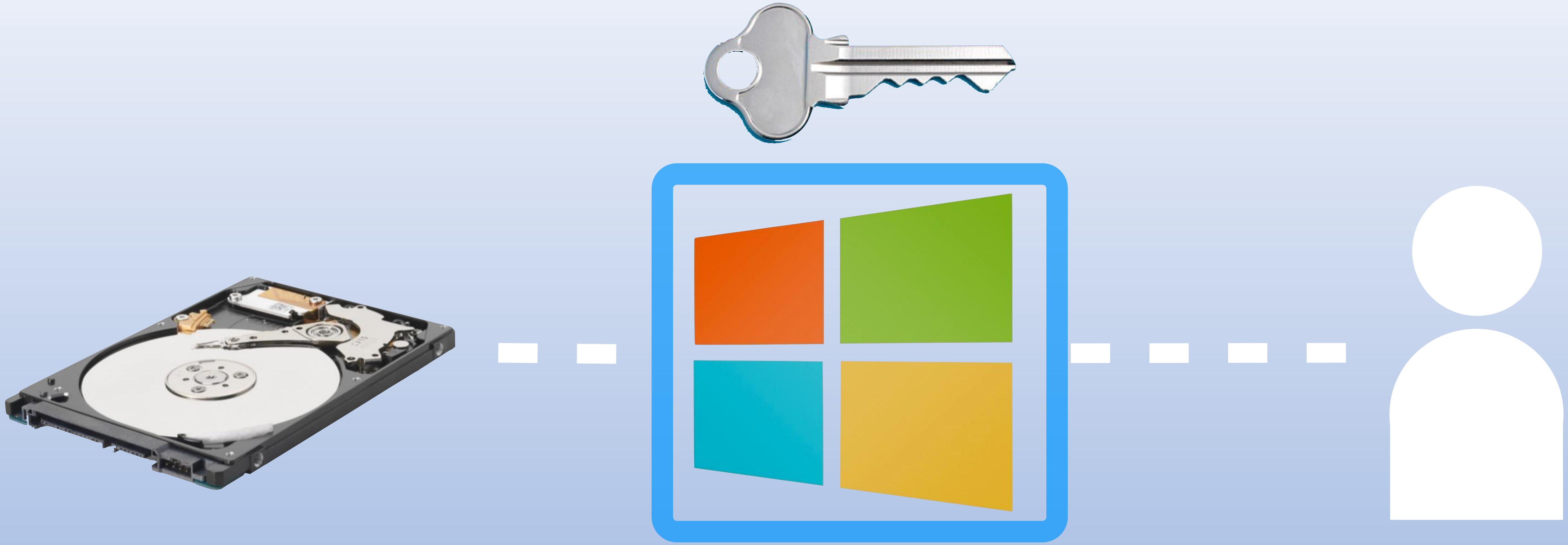
FileVault

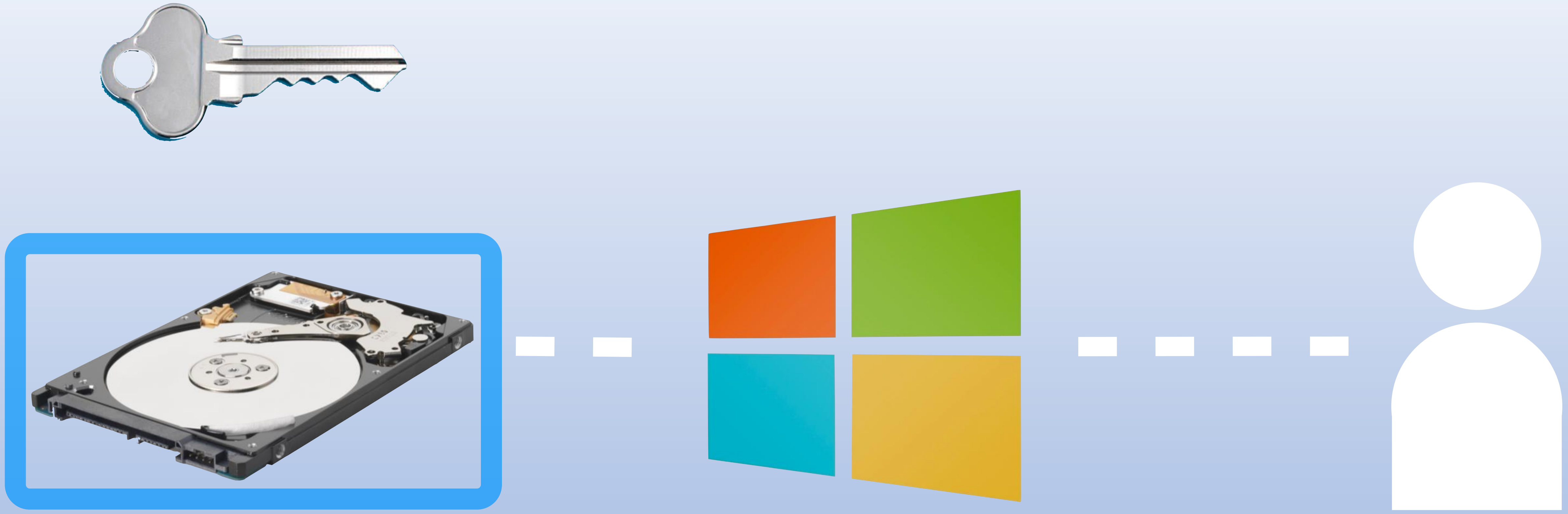
LUKS

Full disk encryption

Uses disk encryption software or hardware to encrypt all data that goes on a disk or disk volume





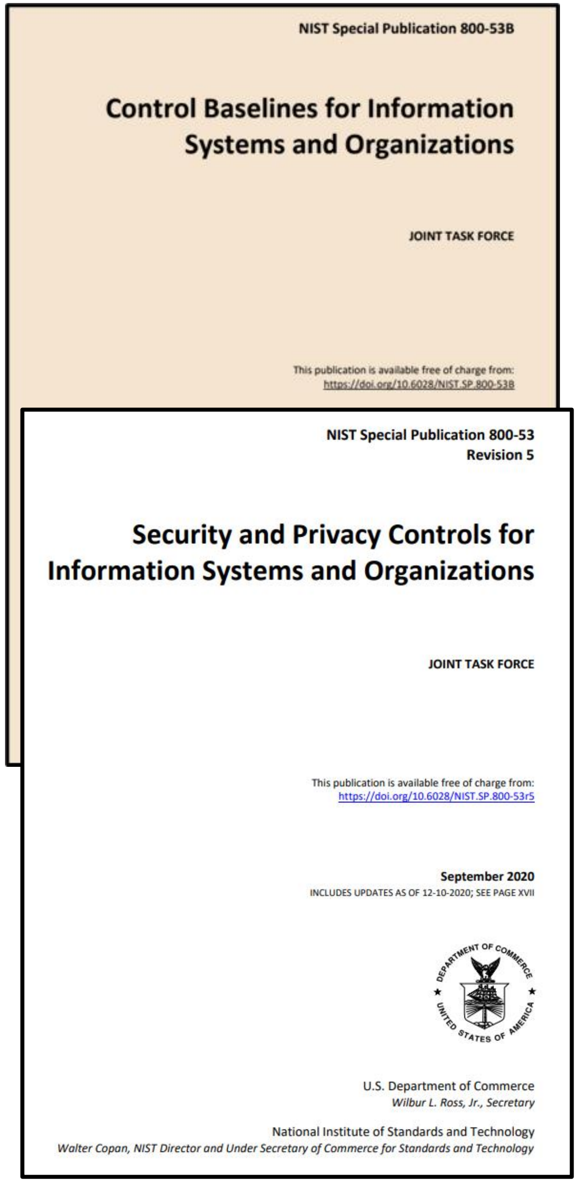


Some disks have built-in encryption

Agenda

- ✓Vulnerabilities and sources of threats
- ✓Physical control inventory baselines
- ✓Perimeter security
- ✓Media protection
- Media sanitization

Cybersecurity Controls



NIST Special Publication 800-53B

Control Baselines for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53B

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

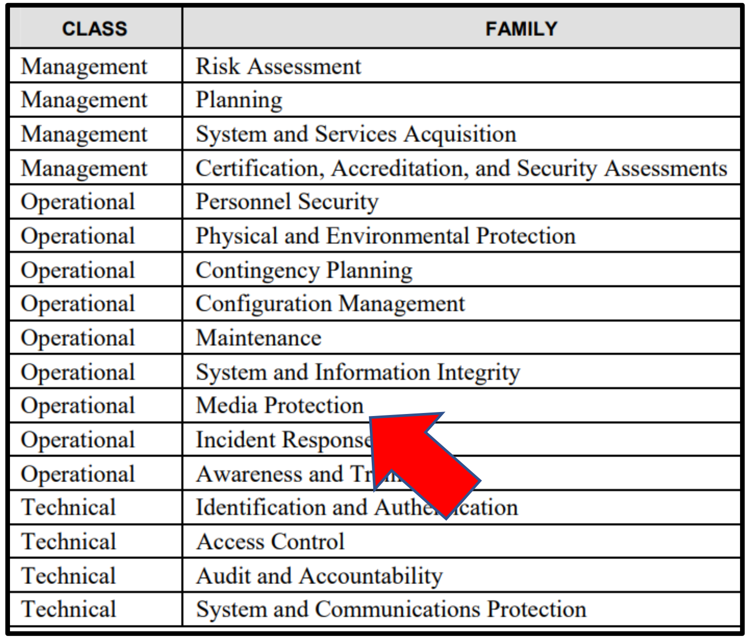
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

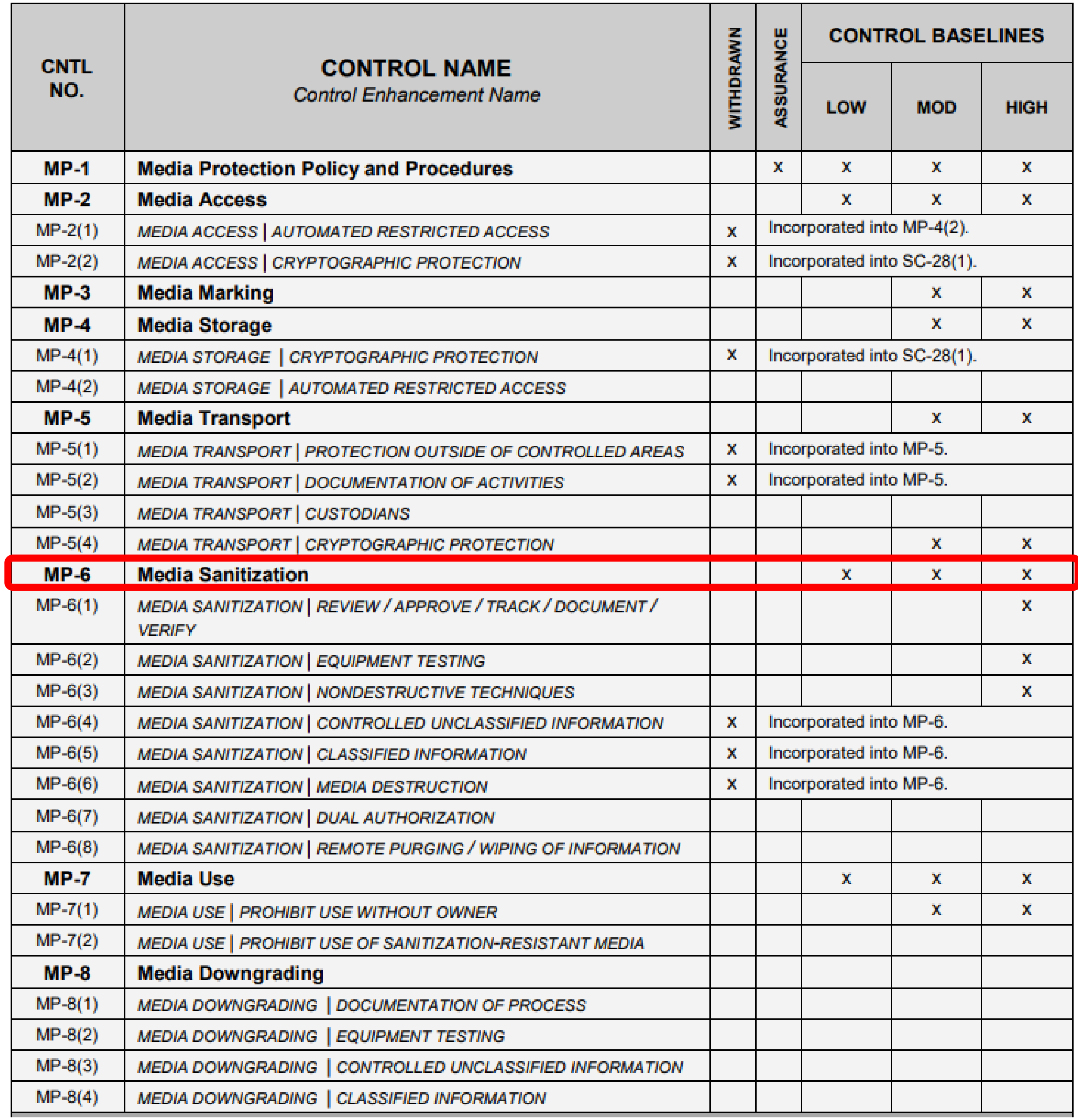
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology



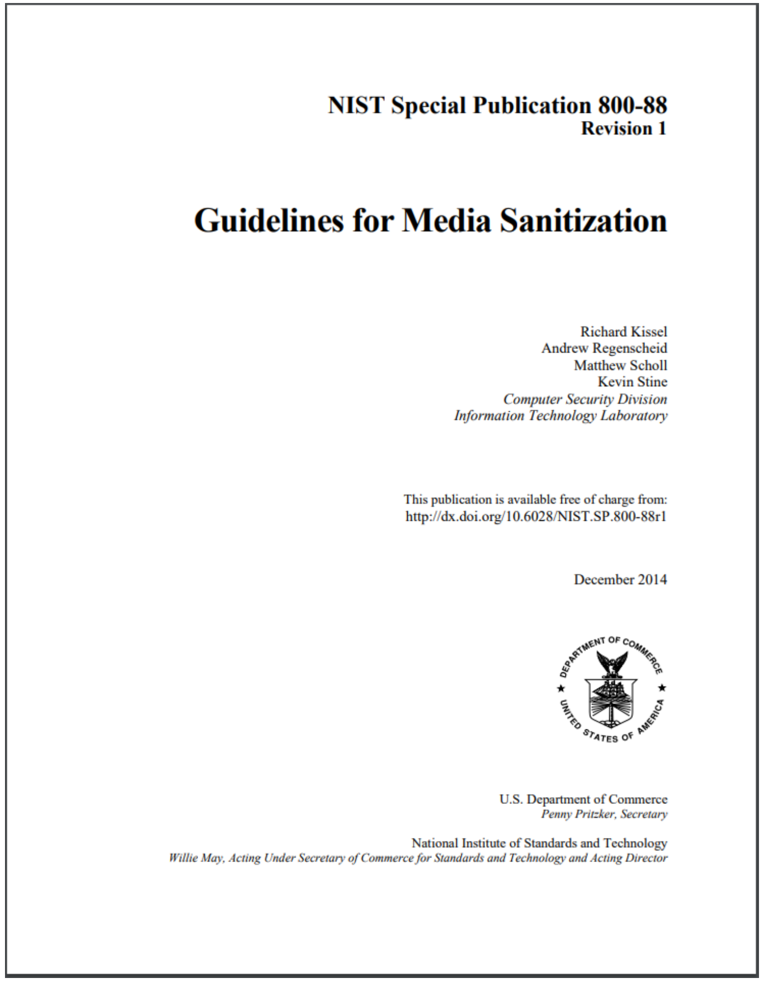
CLASS	FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection



CNTL NO.	CONTROL NAME *Control Enhancement Name*	WITHDRAWN	ASSURANCE	CONTROL BASELINES		
				LOW	MOD	HIGH
MP-1	**Media Protection Policy and Procedures**		x	x	x	x
MP-2	**Media Access**			x	x	x
MP-2(1)	*MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS*	x	Incorporated into MP-4(2).			
MP-2(2)	*MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-3	**Media Marking**				x	x
MP-4	**Media Storage**				x	x
MP-4(1)	*MEDIA STORAGE | CRYPTOGRAPHIC PROTECTION*	x	Incorporated into SC-28(1).			
MP-4(2)	*MEDIA STORAGE | AUTOMATED RESTRICTED ACCESS*					
MP-5	**Media Transport**				x	x
MP-5(1)	*MEDIA TRANSPORT | PROTECTION OUTSIDE OF CONTROLLED AREAS*	x	Incorporated into MP-5.			
MP-5(2)	*MEDIA TRANSPORT | DOCUMENTATION OF ACTIVITIES*	x	Incorporated into MP-5.			
MP-5(3)	*MEDIA TRANSPORT | CUSTODIANS*					
MP-5(4)	*MEDIA TRANSPORT | CRYPTOGRAPHIC PROTECTION*				x	x
MP-6	**Media Sanitization**			x	x	x
MP-6(1)	*MEDIA SANITIZATION | REVIEW / APPROVE / TRACK / DOCUMENT / VERIFY*					x
MP-6(2)	*MEDIA SANITIZATION | EQUIPMENT TESTING*					x
MP-6(3)	*MEDIA SANITIZATION | NONDESTRUCTIVE TECHNIQUES*					x
MP-6(4)	*MEDIA SANITIZATION | CONTROLLED UNCLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(5)	*MEDIA SANITIZATION | CLASSIFIED INFORMATION*	x	Incorporated into MP-6.			
MP-6(6)	*MEDIA SANITIZATION | MEDIA DESTRUCTION*	x	Incorporated into MP-6.			
MP-6(7)	*MEDIA SANITIZATION | DUAL AUTHORIZATION*					
MP-6(8)	*MEDIA SANITIZATION | REMOTE PURGING / WIPING OF INFORMATION*					
MP-7	**Media Use**			x	x	x
MP-7(1)	*MEDIA USE | PROHIBIT USE WITHOUT OWNER*				x	x
MP-7(2)	*MEDIA USE | PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA*					
MP-8	**Media Downgrading**					
MP-8(1)	*MEDIA DOWNGRADING | DOCUMENTATION OF PROCESS*					
MP-8(2)	*MEDIA DOWNGRADING | EQUIPMENT TESTING*					
MP-8(3)	*MEDIA DOWNGRADING | CONTROLLED UNCLASSIFIED INFORMATION*					
MP-8(4)	*MEDIA DOWNGRADING | CLASSIFIED INFORMATION*					

ENERPAC

Media sanitization



NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine
Computer Security Division
Information Technology Laboratory

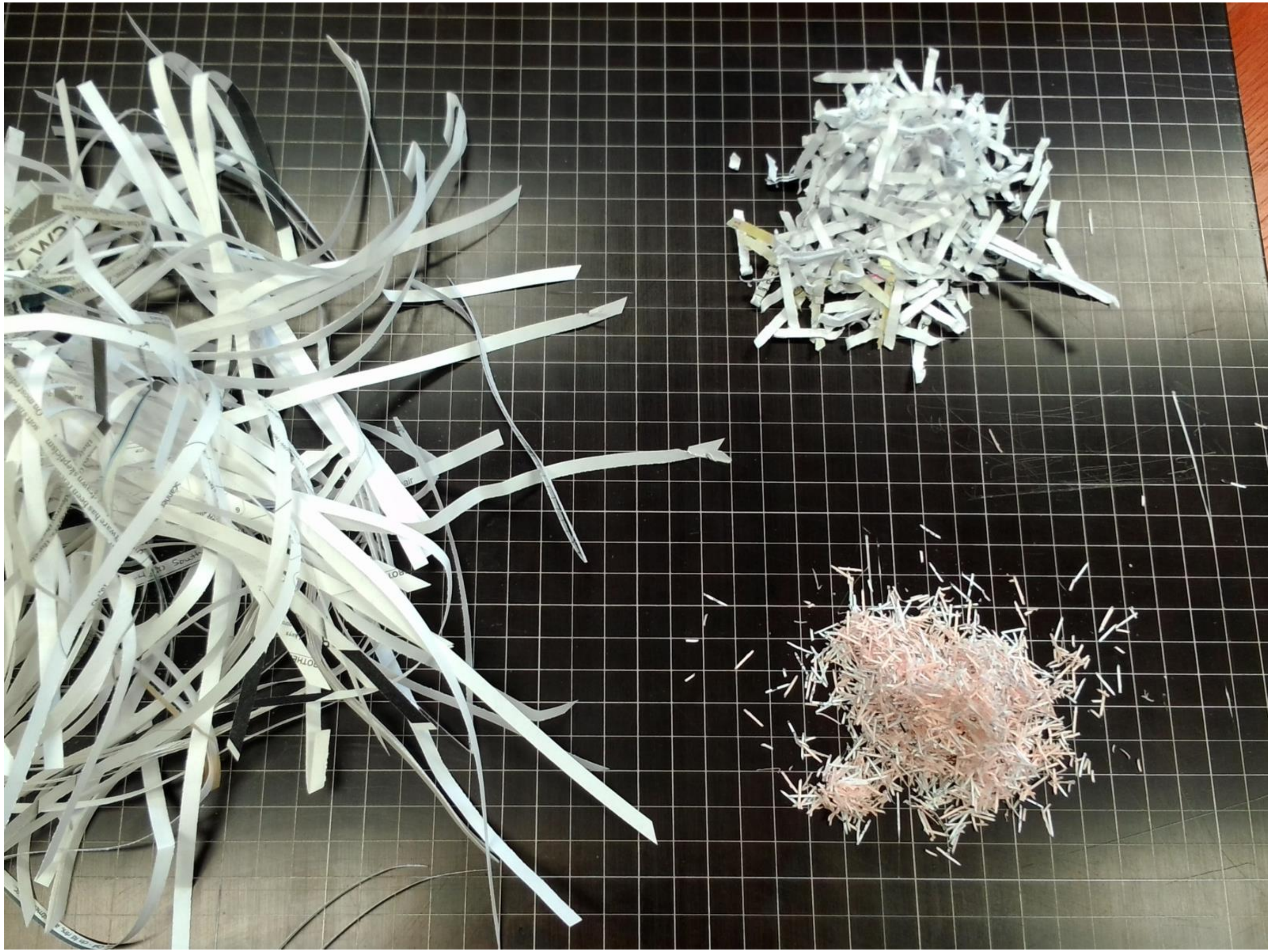
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

December 2014

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director



Paper shredders have different levels of security, above: Levels 1, 3, 6

Agenda

✓Schedule Update

✓Vulnerabilities and sources of threats

✓Physical control inventory baselines

✓Perimeter security

✓Media protection

✓Media sanitization