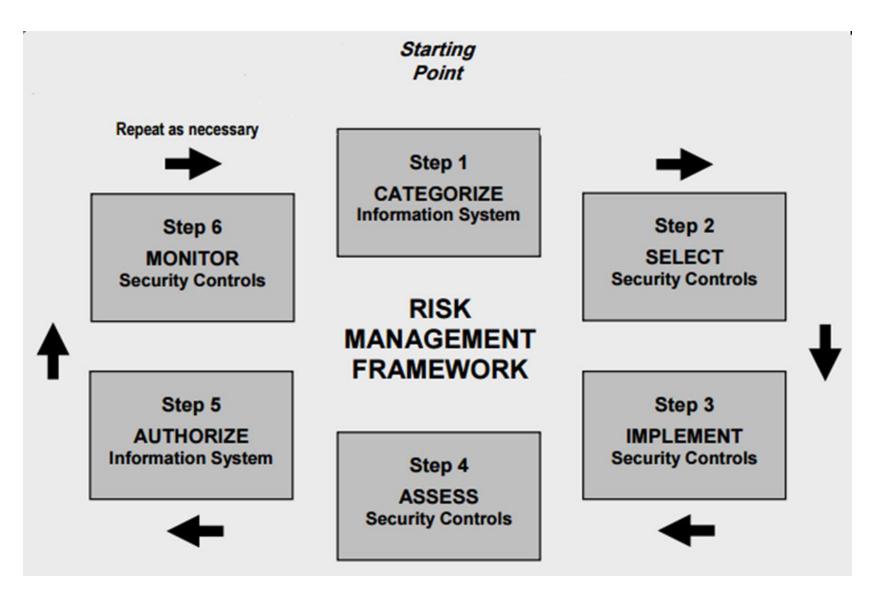
Unit #9

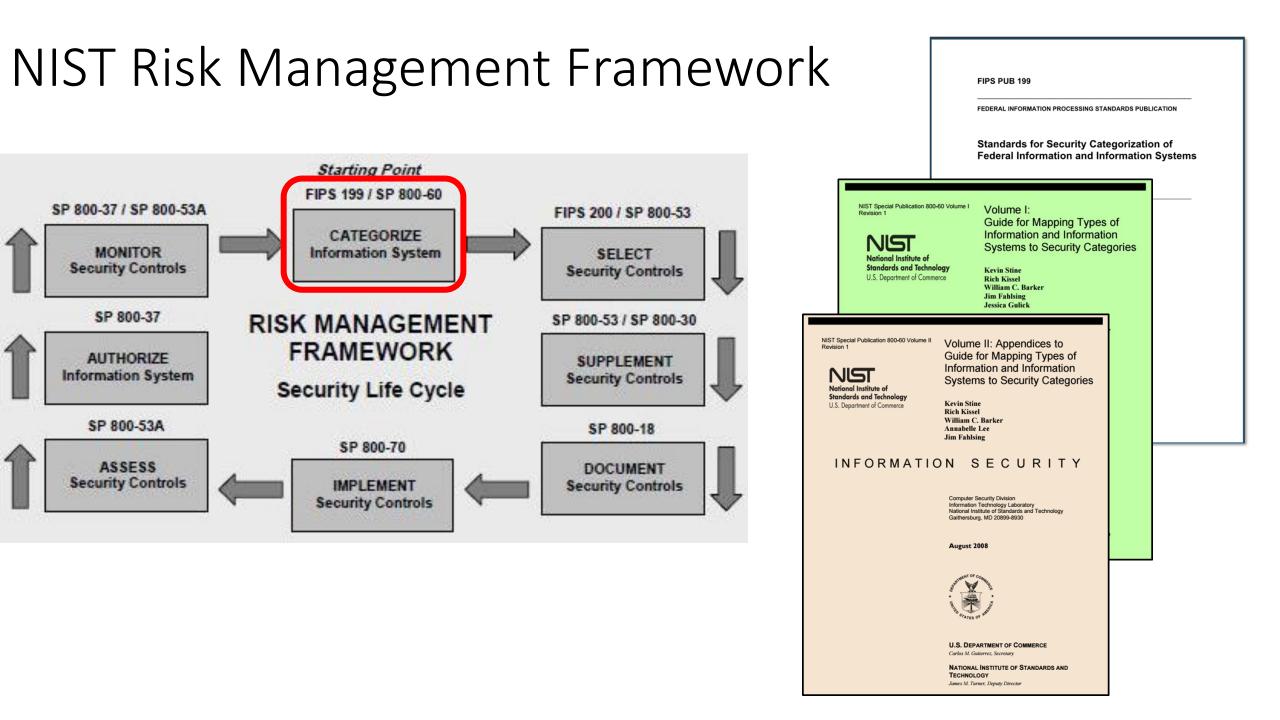
MIS5214

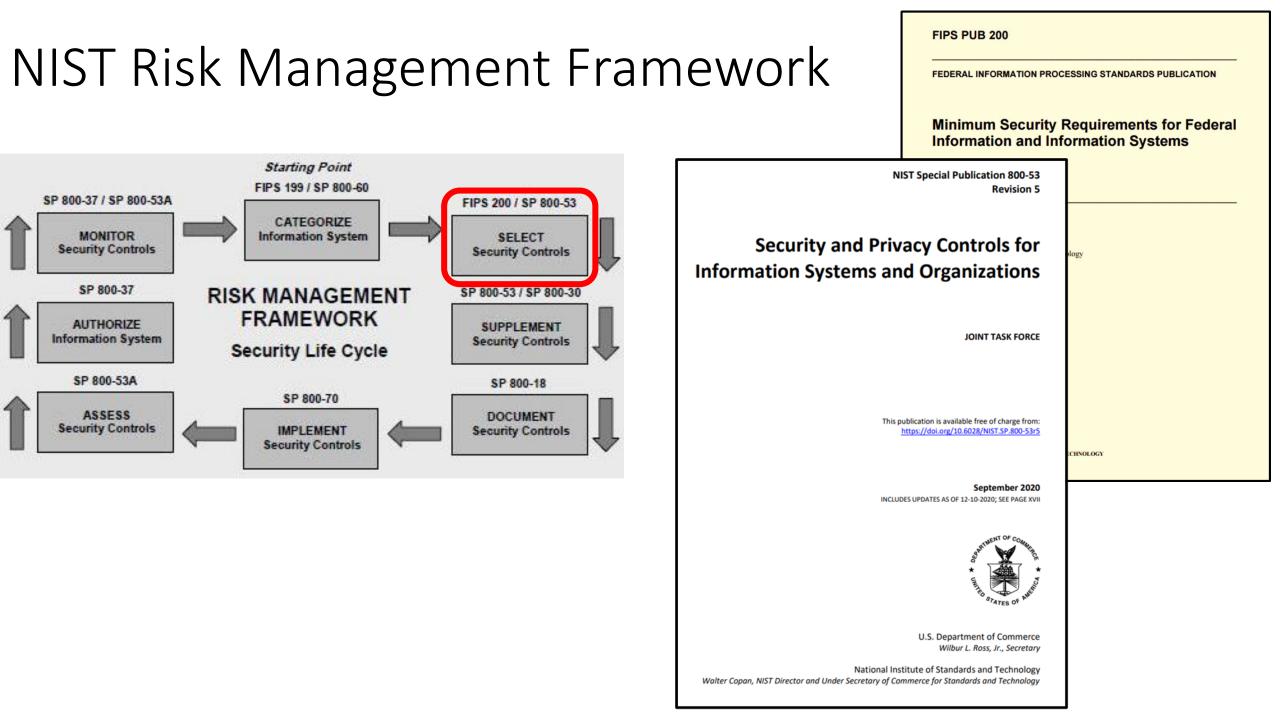
Host Hardening

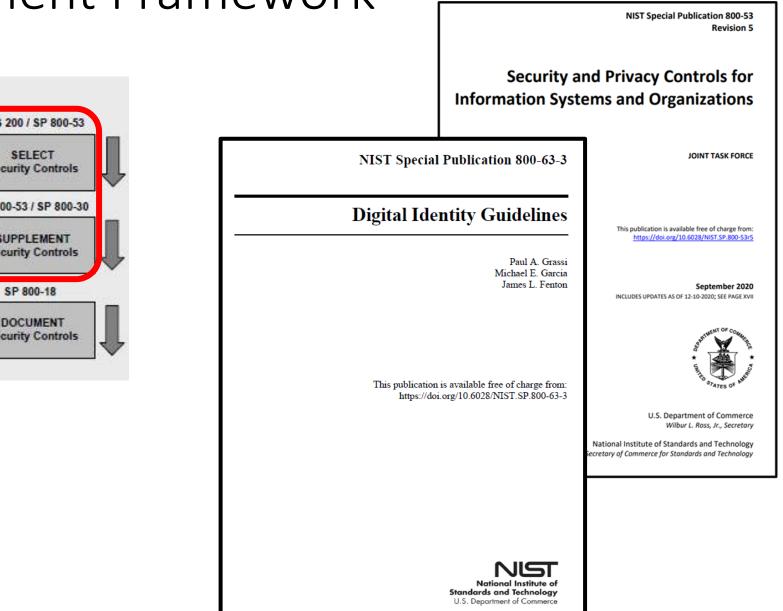
Agenda

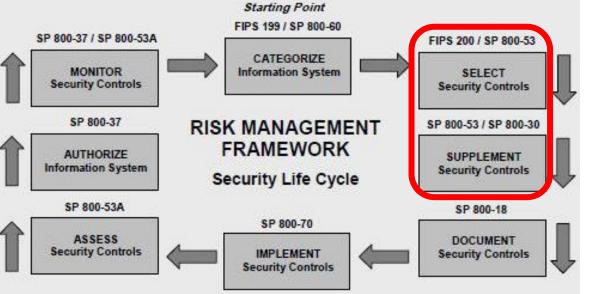
- Risk Management Framework A quick review...
- Implementing controls Host hardening...
 - Security configuration checklist (with STIG Viewer)
- SCAP Security Content Automation Protocol
- System Security Plan's Appendix 1
 - Select 1 Technical control family to fill out for your information system
- System Security Plan's System Information
 - Information System Type
- Team Project SSP draft development...

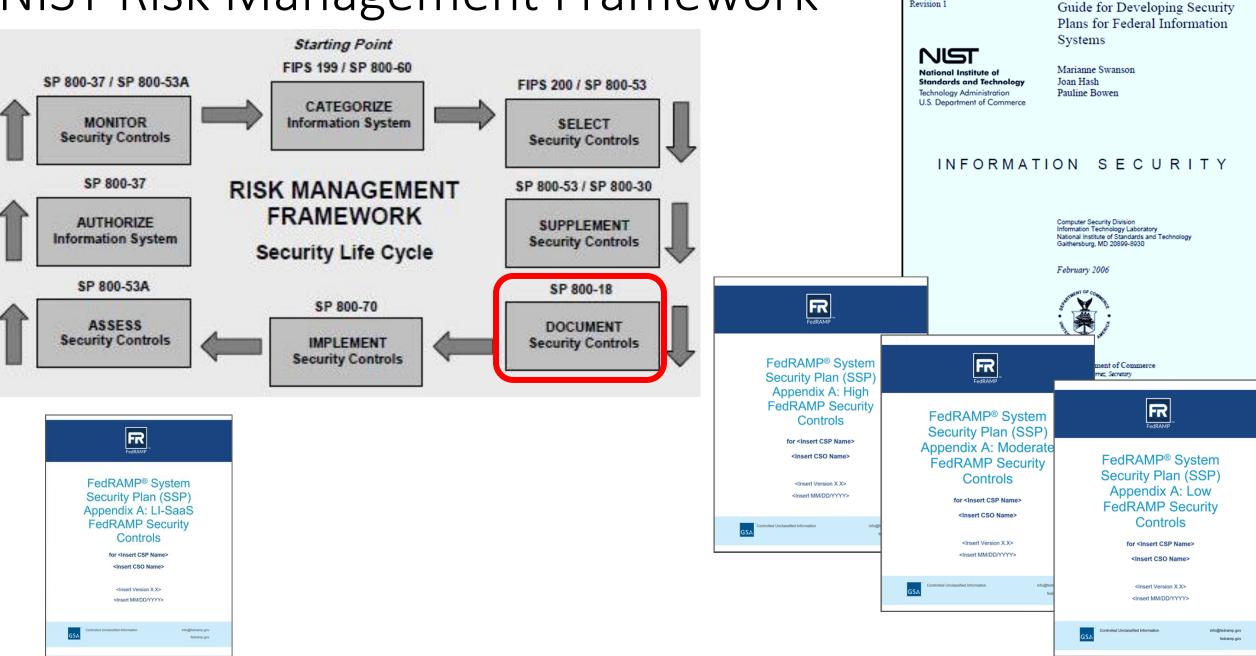






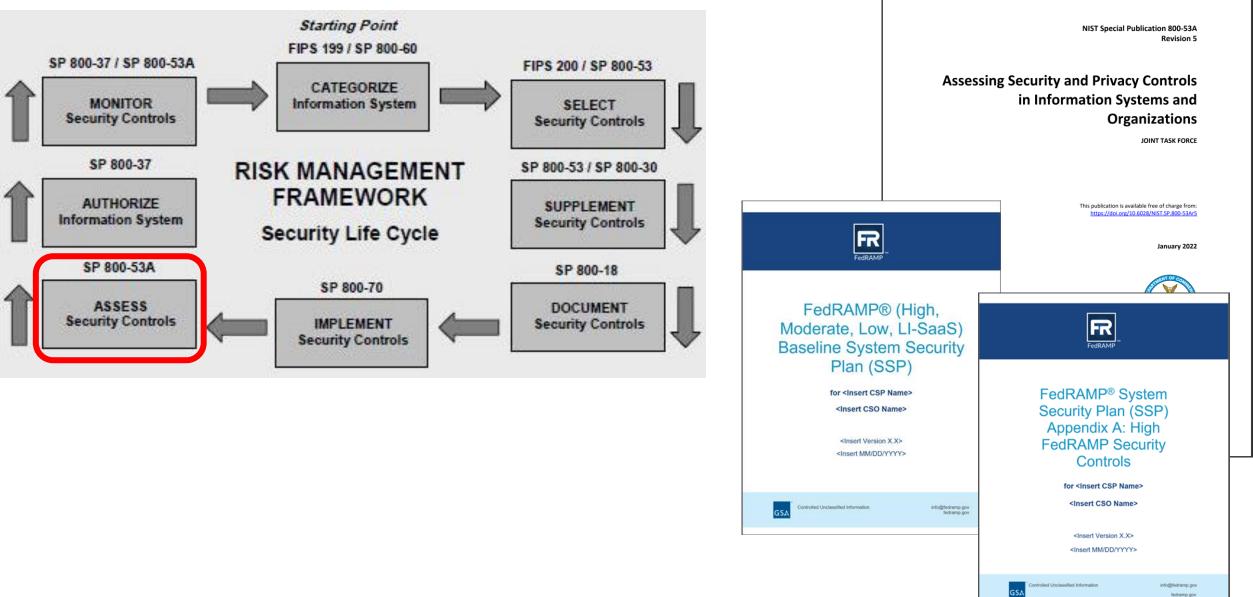






NIST Special Publication 800-18

Revision 1



Which controls aid in Host Hardening... ?

NIST Special Publication 800-18 Revision 1



Guide for Developing Security Plans for Federal Information Systems

National Institute of Standards and Technology Technology Administration U.S. Department of Commerce Marianne Swanson Joan Hash Pauline Bowen

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20890-8930

February 2006



U.S. Department of Commerce Carlos M.Gutierres, Secretary

National Institute of Standards and Technology William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

NIST Special Publication 800-53 Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

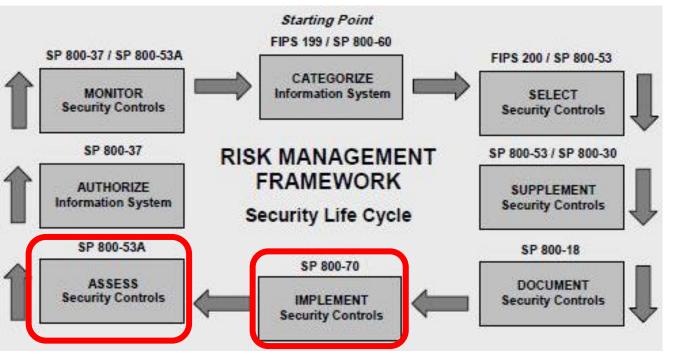
JOINT TASK FORCE TRANSFORMATION INITIATIVE

This publication is available free of charge from: http://dx.doi.org/10.6028/NIST.SP.800-53r4



CNTL		RITY	INITIAL CONTROL BASELINES				
NO.	CONTROL NAME	PRIORITY	LOW	MOD	HIGH		
	Configurati	on Mai	nagement				
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1		
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)		
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)		
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)		
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)		
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)		
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)		
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)		
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9		
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10		
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11		

	Risk Assessment												
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1								
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2								
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3								
RA-4	Withdrawn												
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)								



A security configuration checklist is a document containing instructions or procedures for:

- Configuring an information technology (IT) product to an operational environment
- Verifying that the product has been configured properly
- Identifying unauthorized changes to the product
- Checklists can help you:
 - Minimize the attack surface
 - Reduce vulnerabilities
 - Lessen the impact of successful attacks
 - Identify changes that might otherwise go undetected



National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

> Stephen D. Quinn Murugiah Souppaya Melanie Cook Computer Security Division Information Technology Laboratory

> > Karen Scarfone Scarfone Cybersecurity Clifton, VA

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-70r4

February 2018



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

Two types of checklists

1. Non-Automated



• Designed to be used manually, such as written instructions that describe the steps an administrator should take to secure a system or to verify its security settings

2. Automated

- Used through one or more tools that automatically alter or verify settings based on the contents of the checklist
- Many checklists are written in Extensible Markup Language (XML), and there are special tools that can use the contents of the XML files to check and alter system settings
 - Security Content Automation Protocol (SCAP) is a common example used to express checklist content in a standardized way that can be processed by tools that support SCAP

Security Configuration Checklist

- There is no checklist that can make a system or product 100 percent secure
- Using checklists does not eliminate the need for ongoing security maintenance, such as patch installation
- Using checklists for hardening systems against software flaws (e.g., by applying patches and eliminating unnecessary functionality) and configuring systems securely will typically:
 - Reduce the number of ways in which systems can be attacked
 - Result in greater product security and protection from threats
 - Help verify the configuration of some types of security controls for system assessments

NIST Special Publication 800-70 Revision 4

National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

> Stephen D. Quinn Murugiah Souppaya Melanie Cook Computer Security Division nformation Technology Laboratory

> > Karen Scarfone Scarfone Cybersecurity Clifton, VA

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-704

February 2018



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

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

ISACA is a source of many audit control checklists



UNIX/LINUX Operating System Security Audit Program

Objective—The objective of the UNIX/LINUX Audit program is to provide management with an independent assessment relating to the effectiveness of configuration and security of the UNIX/LINUX operations systems...

FREE to ISACA Members Not a Member? Join Now

AUDIT PROGRAM

AUDIT PROGRAM

Windows Active Directory Audit Program

Objective—The Active Directory audit review will: Provide management with an evaluation of the Active Directory implementation and management security design effectiveness Provide management with an independent...

FREE to ISACA Members Not a Member? Join Now

AUDIT PROGRAM

Network Perimeter Security Audit Program

Objective—The objectives of the network perimeter security audit review are to:Provide management with an independent assessment relating to the effectiveness of the network perimeter security and its alignment with... FREE MEMBER PREVIEW



AUDIT PROGRAM

Secure Shell Protocol (SSH) Audit Program

Objective—Provides enterprises with a means to assess the effectiveness of their use of the SSH protocol, including key management and applicable SSH controls. Scope—The use of the Secure Shell (SSH) protocol...

FREE to ISACA Members Not a Member? Join Now

ISACA	Application au			Q LOGOUT				
ACA	WHY ISACA?	MEMBERSHIP	CREDENTIALING	TRAINING & I	EVENTS	RESOURCES	ENTERPRI	ISE
arch Applicat	tion audit checklist		NO				×	Q
	↓ III III /	Results 17-32 of 132 for J	Application audit checklist				RELEVAN	NCY DATE V
& Assurance mance nation Security ty		ObjectiveT	Is Audit Program The objective of a cyber si as of cyber defense, with a	ecurity audit is to 1 focus on the mp	provide mana ist fundamen	agement with an tai and valuable a	evaluation of th.	e h_
sial Intelligence or and Leadership I Computing	*	ObjectiveT assessment FREE to ISAI Not a Memb	W X Operating System Sec The objective of the UNIX, t relating to the effectiven ICA Members ber? Join Now	/LINUX Audit prog less of configurati	gram is to pro			
l Computing I F Jiance Governance		Domino services and FREE to ISAI Not a Memb	ino Server Audit Program ver comprises a series of connect to remote comp (CA Members ber? Join Now	cooperating proc	esses that co audit planning	mmunicate with g process, the au	one another on ditor must deter	multiple mine the
I Transformation ging Technologies	~	Objective-T relating to th FREE to ISAI Not a Memb	Audit Program The objective of the 2/OS. The controls addressing the ICA Members ber? Join Now	e configuration ar	provide mani nd security of	agement with an the z/OS operate	independent as ons systems wi	sessment th the
Type Article Type ersion	•	Objective – T implemental FREE to ISA	Active Directory Audit Pr The Active Directory audit tion and management se iCA Members ber? Join Now	review will: Provid	de managemi ictiveness Pro	ent with an evalu wide managemer	ation of the Acti nt with an indep-	ive Directory endent
	*	1journal/is	s to Simplify Auditing So stues/2015/volume-4/thr as governance, control, ris	ee-ways-to-simpli	lify-auditing-se	oftware-security-	requirements-ar	nd-design"
		Objective: Pr the process	anagement Audit Program Perform a review of the ch- is controlled, monitored a BER PREVIEW	ange managemer	nt process to e with good pr	provide managen ractices. Format	nent with assur ZIP	ance that
		4 FREE to ISAI Not a Memb	will focus on the acquisiti ad planned, including, but iCA Members ber? Join Now	on, architecture, n not restricted to, p	ollout and set policies, stand	curity of biometri dards and proced	c technologies, lures, as well as	both the resilience
		The primary independent FREE to ISA	A Audit Program voljectives of the biometri t assessment of the effect ICA Members ber? Join Now	ric audit/assuranc tiveness of the ar	ce review are rchitecture an	to: Provide mana id security of the	igement with an deployed biome	etric
		The major of assessment FREE to ISA	at ity Audit Program objectives of the IPv6 netw t of the effectiveness of th ICA Members ber? Join Now					
	-	Objective-T	ile Server Audit Program The objective of the Winde around the enterprise's se	ows File Server Au	udit Program isessment of	is to ensure data the controls arou	confidentiality, i nd Windows File	integrity and e Servers
	100 (married	Objective-T assessment FREE to ISA	and Audit Program The objective of the social trelating to the effectiven (CA Members ber? Join Now	I media Audit revia ress of controls or	ew is to provi ver the enterp	de management rrise's social med	with an indeper la policies and p	ndent processes
		The objectiv Many of the FREE to ISA	or c Audit Program wes of IT strategic manage processes within the IT s (CA Members ber? Join Now	ement can be two strategic manager	ifold: A comp ment audit pri	onent of an IT ge ogram are define	neral controls re d as entity-level	eview controls a
		The objectiv Many of the FREE to ISA	Management Audit Prog ves of the IT tactical mans processes within the IT t ICA Members ber? Join Now	sgement can be ty	wofold: A con ient audit proj	nponent of an IT i gram are defined	general controls as entity-level c	s review controls or
	- 41 in	Objective-P effectivenes FREE to ISA	M nagement Audit Program Provide senior manageme as of the IT risk managem ICA Members ber? Join Now	ent with an unders	standing and a porting frame	assessment of th work and policies	e efficiency and s and assurance	l that IT ris
	10	Objective-P provider's in FREE to ISA	au puting Management Au Provide stakeholders with iternal controls and secur ICA Members ber? Join Now	an assessment o	of the effective al control defi	eness of the clou iciencies within th	id computing se lie customer org	rvice janization
			< 1	2 3 4	5 >			

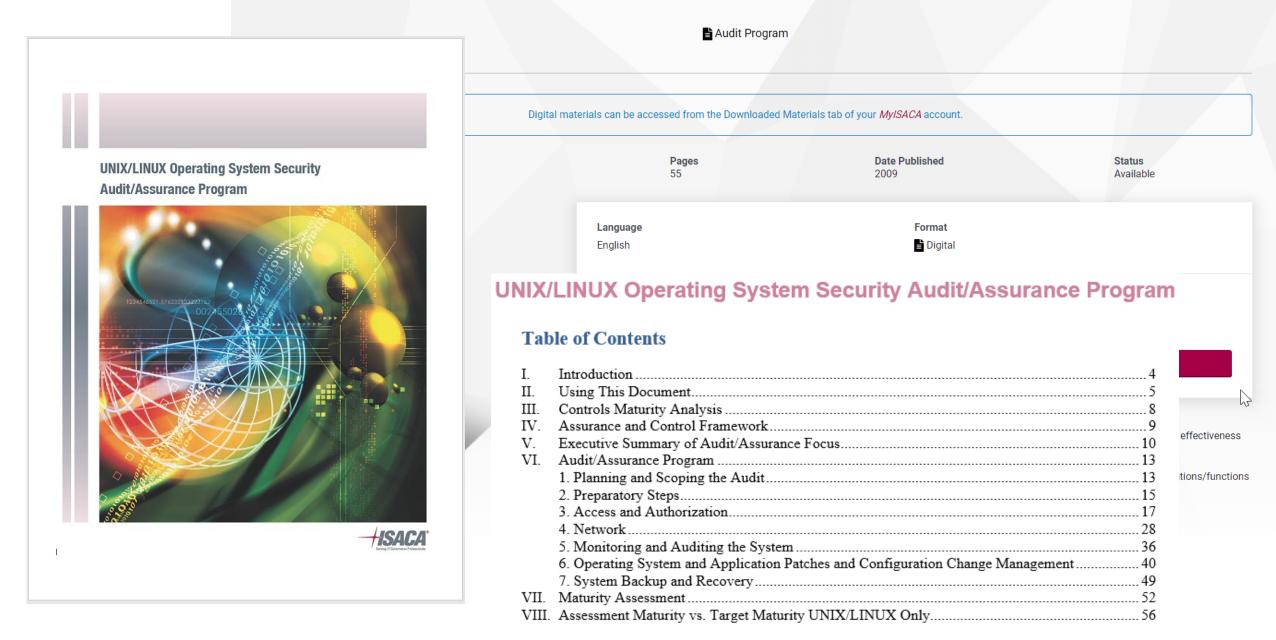
0000 0000

Sea

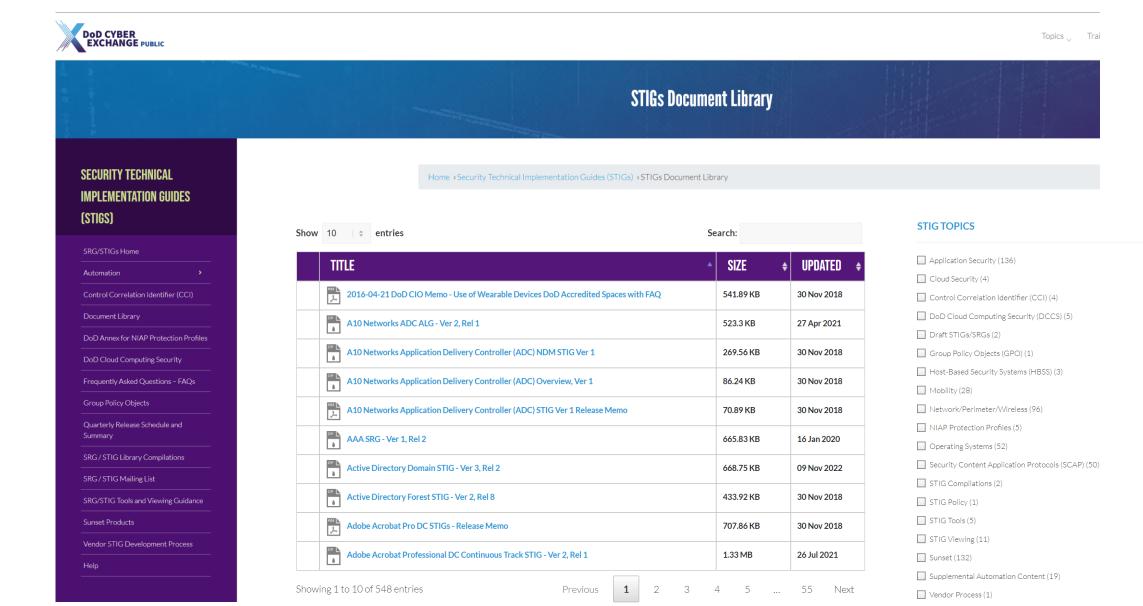
Product

Article Tr

UNIX/LINUX Operating System Security Audit Program



Security Technical Implementation Guides



[+]

[+]

[+]

[+]

[+]

[+]

[+]

[+]

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



Automation

Control Correlation Identifier (CCI)

Document Library

SRG / STIG Mailing List

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 Viewing Tools

Sunset Products

Vendor STIG Development Process

Review (SRR) Tools (scripts and OVAL Benchmarks), Group policy objects, and draft SRGs and STIGs.

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.

Topics 🖉

Training 🖉

PKI/PKE 🖉

SRGs/STIGs

Resources

Help

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.

SRG/STIG Compilations

TITLE	SIZE \$	UPDATED \$
Compilation - SRG-STIG Library	337.46 MB	30 Jan 2024
Compilation - SRG-STIG Library - READ ME	122.17 KB	19 Jun 2019

Help

STIG Viewer

STIG Viewer 3.x

	TITLE	SIZE \$	UPDATED \$
0	Stig Viewer 3 CKLB JSON Schema	2.51 KB	10 Jan 2024
	STIG Viewer 3.3 Hashes	2.08 KB	07 Feb 2024
	STIG Viewer 3.3-Linux	129.63 MB	07 Feb 2024
	STIG Viewer 3.3-Win64	140.36 MB	07 Feb 2024
	STIG Viewer 3.3-Win64 msi	139.4 MB	07 Feb 2024
	STIG Viewer 3.x User Guide - Ver 1, Rel 3	15.84 MB	26 Feb 2024

STIG Viewer 2.17

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
Vendor STIG Acronym List	178.74 KB	16 Jan 2020
	TITLE Image: How to Create and SRG-STIG ID Mapping Spreadsheet Image: STIG Sorted by STIG ID Image: STIG Sorted by Vulnerability ID Image: STIG Viewer 2.17 Image: STIG Viewer 2.17 Hashes Image: STIG Viewer 2.17 Linux Image: STIG Viewer 2.17-Win64 Image: STIG Viewer 2.17-Win64 msi	How to Create and SRG-STIG ID Mapping Spreadsheet298.21 KBSTIG Sorted by STIG ID103.46 KBSTIG Sorted by Vulnerability ID101.59 KBSTIG Viewer 2.171.14 MBSTIG Viewer 2.17 Hashes1.36 KBSTIG Viewer 2.17-Linux73.38 MBSTIG Viewer 2.17-Winó454.03 MBSTIG Viewer 2.17-Winó4 msi54.26 MB

😰 DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

▼ STIGs			Rule ID	Rule Name	Authentication, Authorization, and Accounting Services (AAA) Security Requirements Guide :: Version 1, Release: 2					
ilter on STIG name		V-80815	SV-95525r1_rule	e SRG-APP-0001	Benchmark Date: 24 Jan 2020					
CK Name	+	V-80817	SV-95527r1_rule	e SRG-APP-0001	Vul ID: V-80817 Rule ID: SV-95527r1_rule STIG ID: SRG-APP-000142-AAA-000020					
A10 Networks ADC ALG Security Technical Implemen	tation Guide	V-80819	SV-95529r1_rule	e SRG-APP-0000	Severity: CAT I Classification: Unclass					
A10 Networks ADC NDM Security Technical Impleme		V-80821	SV-95531r1_rule	e SRG-APP-0000						
 Authentication, Authorization, and Accounting Service 		V-80823	SV-95533r1_rule	e SRG-APP-0002						
Active Directory Domain Security Technical Implemer	ntation Guide	V-80825	SV-95535r1_rule	e SRG-APP-0002						
Active Directory Forest Security Technical Implementa		V-80827	SV-95537r1_rule	e SRG-APP-0000	Group Title: SRG-APP-000142-AAA-000020					
Adobe Acrobat Professional DC Continuous Track Sec	curity Techn	V-80829	SV-95539r1_rule	e SRG-APP-0000						
Adobe Acrobat Reader DC Continuous Track Security	Technical I	V-80831	SV-95541r1_rule	e SRG-APP-0000	Rule Title : AAA Services must be configured to use protocols that encrypt credentials when authenticating clients, as defined in PPSM CAL and vulnerability assessments.					
Akamai KSD Service Impact Level 2 ALG Security Tech	nnical Imple	V-80833	SV-95543r1_rule	e SRG-APP-0000						
Akamai KSD Service Impact Level 2 NDM Security Tec	chnical Impl	V-80835	SV-95545r1_rule	e SRG-APP-0000	Discussion: Authentication protection of the client credentials (specifically the password or shared secret) prevents unauthorize					
APACHE 2.2 Server for UNIX Security Technical Imple	mentation	V-80837	SV-95547r1_rule	e SRG-APP-0002	access to resources. The RADIUS protocol encrypts the password field in the access-request packet, from the client to the AAA server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting,					
APACHE 2.2 Site for UNIX Security Technical Implement	entation Gui	V-80839	SV-95549r1_rule	e SRG-APP-0002	be captured by a third-party. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within t					
APACHE 2.2 Server for Windows Security Technical Im	nplementati 🗸	V-80841	SV-95551r1_rule	e SRG-APP-0002	header is a field that indicates whether the body is encrypted or not. Other protocols have similar protections. When unencrypt credentials are passed, adversaries can gain access to resources.					
Profile: No Profile 🔹		V-80843	SV-95553r1_rule	e SRG-APP-0002						
		V-80845	SV-95555r1_rule	e SRG-APP-0003	Check Text : Verify AAA Services are configured to use protocols that encrypt credentials when authenticating clients. Both the					
Filter Panel		V-80847	SV-95557r1_rule	e SRG-APP-0003	RADIUS and TACACS+ protocols are acceptable when configured to perform encryption. For any protocol implemented, CAL and vulnerability assessments must be reviewed to ensure the protocols are properly configured.					
Must match: All Any		V-80849	SV-95559r1_rule	e SRG-APP-0003						
Keyword Enter filter keyword Inclusive (+) Filter Exclusive (-) Filter	Add	V-80851	SV-95561r1_rule	e SRG-APP-0000	If AAA Services are not configured to use protocols that encrypt credentials when authenticating clients, as defined in the PPSM CAL and vulnerability assessments, this is a finding.					
+ / - Keyword	Filter	V-80855	SV-95565r1_rule	e SRG-APP-0003						
+ / - Кеумоги	Titter	V-80857	SV-95567r1_rule	e SRG-APP-0000	Fix Text : Configure AAA Services to use protocols that encrypt credentials when authenticating clients. Both the RADIUS and TACACS+ protocols are acceptable when configured to perform encryption. For any protocol implemented, the PPSM CAL and					
		V-80859	SV-95569r1_rule	e SRG-APP-0000	vulnerability assessments must be reviewed to ensure the protocols are properly configured.					
		V-80861	SV-95571r1_rule	e SRG-APP-0000						
		V-80863	SV-95573r1_rule	e SRG-APP-0000	References					
		V-80865	SV-95575r1_rule	e SRG-APP-0000	CCI : CCI-000382: The organization configures the information system to prohibit or restrict the use of organization defined					
		V-80867	SV-95577r1_rule	e SRG-APP-0001	functions, ports, protocols, and/or services. NIST SP 800-53 :: CM-7					
No content in table		V-80869	SV-95579r1_rule	e SRG-APP-0003	NIST SP 800-53A :: CM-7.1 (iii)					
		V-80871	SV-95581r2_rule	e SRG-APP-0001	NIST SP 800-53 Revision 4 :: CM-7 b					
		V-80873	SV-95583r1_rule	e SRG-APP-0001						
\triangleright		V-80875	SV-95585r1_rule	e SRG-APP-0001						
-		V-80877	SV-95587r1_rule	e SRG-APP-0001						
		V-80879	V-80879 SV-95589r1_rule SRG-APP-0003							
Remove Filter(s) Remove All Filters		V-80881	SV-95591r1_rule	e SRG-APP-0003						
hemove riter(s)		Showing rule 2	out of 164							

😰 DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

7 STIGs	Vul ID	Rule ID	Rule Name	Microsoft Windows 11 Security Technical Implementation Guide :: Version 1, Release: 2 Benchmark Date: 14 Nov 2022						
Windows	V-253254	SV-253254r82	SRG-OS-00048	Vul ID: V-253254 Rule ID: SV-253254r828846_rule STIG ID: WN11-00-000005						
CK Name +	V-253255	SV-253255r82	SRG-OS-00042	Severity: CAT II Classification: Unclass						
APACHE 2.2 Server for Windows Security Technical Implementati	V-253256	SV-253256r82	SRG-OS-00042							
APACHE 2.2 Site for Windows Security Technical Implementation	V-253257	SV-253257r82	SRG-OS-00042							
Apache Server 2.4 Windows Server Security Technical Implement	V-253258	SV-253258r82	SRG-OS-00019							
Apache Server 2.4 Windows Site Security Technical Implementati	V-253259	SV-253259r82	SRG-OS-00040							
Citrix Virtual Apps and Desktop 7.x Windows Virtual Delivery Age	V-253260	SV-253260r82	SRG-OS-00040	Group Title: SRG-OS-000480-GPOS-00227						
Citrix XenDesktop 7.x Windows Virtual Delivery Agent Security T	V-253261	SV-253261r82	SRG-OS-00012							
EDB Postgres Advanced Server v11 on Windows Security Technic	V-253262	SV-253262r82	SRG-OS-00037	Rule Title: Domain-joined systems must use Windows 11 Enterprise Edition 64-bit version.						
Google Chrome Current Windows Security Technical Implementa	V-253263	SV-253263r82	SRG-OS-00048	Discussion : Features such as Credential Guard use virtualization-based security to protect information that could be used in						
 Microsoft Windows 10 Security Technical Implementation Guide 	V-253264	SV-253264r82	SRG-OS-00048	credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Gua						
Microsoft Windows 11 Security Technical Implementation Guide	V-253265	SV-253265r82	SRG-OS-00008	to be configured and enabled properly. Virtualization-based security and Credential Guard are only available with Windows 11 Enterprise 64-bit version.						
Microsoft Windows Server 2012/2012 R2 Domain Controller Sec	V-253266	SV-253266r82	SRG-OS-00048							
Microsoft Windows Server 2012/2012 R2 Member Server Securit	V-253267	SV-253267r82	SRG-OS-00013	Check Text: Verify domain-joined systems are using Windows 11 Enterprise Edition 64-bit version.						
Profile: No Profile 🔹	V-253268	SV-253268r82	SRG-OS-00046	For standalone systems, this is NA.						
	V-253269	SV-253269r82	SRG-OS-00031							
Filter Panel	V-253270	SV-253270r82	SRG-OS-00048	Open "Settings".						
Must match: All Any	V-253271	SV-253271r82	SRG-OS-00031	Select "System", then "About".						
Keyword Enter filter keyword Add	V-253272	SV-253272r82	SRG-OS-00048							
Inclusive (+) Filter Exclusive (-) Filter	V-253273	SV-253273r82	SRG-OS-00007	If "Edition" is not "Windows 11 Enterprise", this is a finding.						
+ / - Keyword Filter	V-253274	SV-253274r84	SRG-OS-00031	If "System type" is not "64-bit operating system", this is a finding.						
45	V-253275	SV-253275r82	SRG-OS-00009	Fix Text : Use Windows 11 Enterprise 64-bit version for domain-joined systems.						
	V-253276	SV-253276r82	SRG-OS-00009	The Text. Ose Windows TT Enterprise of bit version for domain joined systems.						
	V-253277	SV-253277r82	SRG-OS-00009	References						
	V-253278	SV-253278r82	SRG-OS-00009	CCI: CCI-000366: The organization implements the security configuration settings.						
	V-253279	SV-253279r82	SRG-OS-00009	NIST SP 800-53 :: CM-6 b						
No content in table	V-253280	SV-253280r82	SRG-OS-00048	NIST SP 800-53A :: CM-6.1 (iv) NIST SP 800-53 Revision 4 :: CM-6 b						
	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							
Remove Filter(s) Remove All Filters	Showing rule 1	out of 252	~							

DISA STIG Viewer : 2.15 : STIG Explorer

File Export Checklist Options Help

STIGs	Vul ID	Rule ID	Rule Name	Windows 10 Security Technical Implementation Guide :: Version 2, Release: 3 Benchmark Date: 01 Nov 2021								
windows 10	V-220697	SV-220697r569187	SRG-OS-000480-GP	Vul ID: V-220697 Rule ID: SV-220697r569187_rule STIG ID: WN10-00-000005								
CK Name	+ V-220698	SV-220698r569187	SRG-OS-000480-GP	Severity: CAT II Classification: Unclass Legacy IDs: V-63319; SV-77809								
Microsoft Windows 10 Mobile Security Technical Implementation Guide	V-220699	SV-220699r569187	SRG-OS-000480-GP									
Windows 10 Security Technical Implementation Guide	V-220700	SV-220700r569187	SRG-OS-000480-GP									
Windows 10 Security Technical Implementation Guide	V-220701	SV-220701r793197	SRG-OS-000191-GP									
✓ Windows 10 Security Technical Implementation Guide	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	Comment Titles CDC OC 000400 CDOC 00007								
	V-220709	SV-220709r569187	SRG-OS-000480-GP	Group Title: SRG-OS-000480-GPOS-00227								
	V-220710	SV-220710r569187	SRG-OS-000138-GP	Rule Title: Domain-joined systems must use Windows 10 Enterprise Edition 64-bit version.								
	V-220711	SV-220711r569187	SRG-OS-000118-GP	Discussion : Footures such as Cradential Cuard use vistualization based essentiate to protect information that sould be used in gradential t								
	V-220712	SV-220712r569187	SRG-OS-000324-GP	Discussion: Features such as Credential Guard use virtualization based security to protect information that could be used in credential t attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured ar								
	V-220713	SV-220713r569187	SRG-OS-000480-GP	enabled properly. Virtualization based security and Credential Guard are only available with Windows 10 Enterprise 64-bit version.								
Profile: No Profile 🔹	V-220714	SV-220714r569187	SRG-OS-000095-GP	Check Text: Verify domain-joined systems are using Windows 10 Enterprise Edition 64-bit version.								
Profile: No Profile +	V-220715	SV-220715r569187	SRG-OS-000480-GP	For standalone systems, this is NA.								
Filter Panel	V-220716	SV-220716r569187	SRG-OS-000076-GP									
Must match: All Any	V-220717	SV-220717r569187	SRG-OS-000312-GP	Open "Settings".								
CATI - CATI Add	V-220718	SV-220718r569187	SRG-OS-000095-GP									
Inclusive (+) Filter Exclusive (-) Filter	V-220719	SV-220719r569187	SRG-OS-000096-GP	Select "System", then "About".								
+ / - Keyword Filter	V-220720	SV-220720r569187	SRG-OS-000095-GP	If "Edition" is not "Windows 10 Enterprise", this is a finding.								
	V-220721	SV-220721r569187	SRG-OS-000096-GP									
	V-220722	SV-220722r569187	SRG-OS-000096-GP	If "System type" is not "64-bit operating system", this is a finding.								
	V-220723	SV-220723r569187	SRG-OS-000480-GP	Fix Text: Use Windows 10 Enterprise 64-bit version for domain-joined systems.								
	V-220724	SV-220724r569187	SRG-OS-000480-GP	D. /								
	V-220725	SV-220725r569187	SRG-OS-000480-GP	References								
	V-220726	SV-220726r569187	SRG-OS-000433-GP	CCI: CCI-000366: The organization implements the security configuration settings.								
	V-220727	SV-220727r569187	SRG-OS-000433-GP	NIST SP 800-53 :: CM-6 b NIST SP 800-53A :: CM-6.1 (iv)								
No content in table	V-220728	SV-220728r569187	SRG-OS-000095-GP	NIST SP 800-53 Revision 4 :: CM-6 b								
	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									

DISA STIG Viewer : 2.7

File	Export	Check	klist	Options	Help								Firewall Security Technical In
Impor	t STIG		🛞 DI	SA STIG Viewer	: 2.7								Firewall Security Technical In
Exit	5		_		Checklist	Options Help	-	_	-	-			IBM DataPower ALG Security
СК			▼ ST	Explorer IGs									IBM DataPower Network Dev
			СК		obat Bra V	Name Cocurity Tochnico	Limpi	amantat			+		Intrusion Detection and Prev
				McAfee Vir	us CK				lame	СК			IPSec VPN Gateway Security
				McAfee Vir	\cup	Microsoft O Microsoft Po	10000	General P	urpose		Tanium 6.5 Tanium 7.0		Juniper SRX SG ALG Security
				McAfee Vir		Microsoft Pr	m	Apple OS	X 10.1		Database S		Juniper SRX SG IDPS Security
				McAfee MC		Microsoft Pu		Apple OS	Sector Con-		IBM DB2 V		Juniper SRX SG NDM Securit
				McAfee MC	-	Microsoft Sł		MAC OSX Apple OS			Microsoft S		Juniper SRX SG VPN Security
				McAfee MC	\cup	Microsoft Vi		Apple OS	0.000000		MS SQL Se		Palo Alto Networks ALG Seco
				McAfee MC		Microsoft W		Apple OS			MS SQL Se		Palo Alto Networks IDPS Sec
				McAfee VS		Microsoft A		AIX 6.1 SE SUSE Linu			Oracle Dat	\square	Palo Alto Networks NDM Se
						Microsoft O	0	IBM Hardy					11g Instance STIG
						Microsoft O		IBM Hard	ware N				12c Security Technical Implementati
						Microsoft O		z/OS ACF			-		anced Server Security Technical Imp
					\square	Microsoft Oi					-D for ACF2		11

CK Name nplementation Guide - Ci... nplementation Guide / Technical Implementati... vice Management Securit... ention Systems (IDPS) Se... Technical Implementatio... Technical Implementatio... y Technical Implementati... y Technical Implementati... / Technical Implementati... urity Technical Implement... urity Technical Implemen... curity Technical Impleme...

Severity Category Code (CAT) Levels

The risk level associated with the information assurance (IA) security weakness and the urgency for a corrective action to be completed

- CAT I Severity Code is assigned to *findings* that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges
 - CAT I weaknesses **must be corrected** before an Authorization to Operate (ATO) is granted
- CAT II Severity Code is assigned to *findings* that have a potential to lead to unauthorized system access or activity.
 - CAT II findings shall be corrected or satisfactorily mitigated before an Authorization to Operate will be granted.
 - A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.
- **CAT III Severity Code** is assigned to recommendations that will improve IA posture but are **not required** for an authorization to operate

DISA STIG Viewer : 2.9.1 : STIG Explorer

File Export Checklist Options Help

DISA STIG Viewer : 2.9.1 : STIG Explorer

File Export Checklist Options Help

e Export Checklist Options Help					
G Explorer			STIG Explorer		
STIGs	Vul ID	Rule Name	▼ STIGs	Vul ID	Rule Name
ilter on STIG name	V-63319	WN10-00-000005	Filter on STIG name	V-63325	WN10-CC-000315
K Name	• V-63321	WN10-CC-000310	CK Name +	V-63335	WN10-CC-000330
voice video session management security kequirements Guide	V-63323	WN10-00-000010	Voice video session management security kequirements duide	V-63347	WN10-CC-000345
vRealize - Cassandra Security Technical Implementation Guide	V-63325	WN10-CC-000315	vRealize - Cassandra Security Technical Implementation Guide	V-63349	WN10-00-000040
Web Policy STIG	V-63329	WN10-CC-000320	Web Policy STIG	V-63351	WN10-00-000045
Web Server Security Requirements Guide	V-63333	WN10-CC-000325	Web Server Security Requirements Guide	V-63353	WN10-00-000050
Windows 10 Security Technical Implementation Guide	V-63335	WN10-CC-000330	Windows 10 Security Technical Implementation Guide	V-63361	WN10-00-000070
Windows 10 Security Technical Implementation Guide	V-63337	WN10-00-000030	Windows 10 Security Technical Implementation Guide	V-63377	WN10-00-000100
Windows 2008 Domain Controller Security Technical Implementation Guide	V-63339	WN10-CC-000335	Windows 2008 Domain Controller Security Technical Implementation Guide	V-63429	WN10-AC-000045
Windows 2008 Domain Controller Security Technical Implementation Guide	V-63341	WN10-CC-000360	Windows 2008 Domain Controller Security Technical Implementation Guide	V-63651	WN10-CC-000155
Windows 2008 Member Server Security Technical Implementation Guide	V-63343	WN10-00-000025	Windows 2008 Member Server Security Technical Implementation Guide	V-63667	WN10-CC-000180
Windows 2008 Member Server Security Technical Implementation Guide	V-63345	WN10-00-000035	Windows 2008 Member Server Security Technical Implementation Guide	V-63671	WN10-CC-000185
Windows 8/8.1 Security Technical Implementation Guide	V-63347	WN10-CC-000345	Windows 8/8.1 Security Technical Implementation Guide	V-63673	WN10-CC-000190
Windows Firewall with Advanced Security Security Technical Implementation Guide	V-63349	WN10-00-000040	Windows Firewall with Advanced Security Security Technical Implementation Guide	V-63739	WN10-SO-000140
Windows PAW Security Technical Implementation Guide	V-63351	WN10-00-000045	Windows PAW Security Technical Implementation Guide	V-63745	WN10-SO-000145
Windows PAW Security Technical Implementation Guide	V-63353	WN10-00-000050	Windows PAW Security Technical Implementation Guide	V-63749	WN10-SO-000150
) >	V-63355	WN10-00-000055		V-63759	WN10-SO-000165
Profile	V-63357	WN10-00-000060	Profile: No Profile 👻	V-63797	WN10-SO-000195
er Panel	V-63359	WN10-00-000065	▼ Filter Panel	V-63801	WN10-SO-000205
Must match: All Any	V-63361	WN10-00-000070	Must match: All Any	V-63847	WN10-UR-000015
Keyword Enter filter keyword Add	V-63363	WN10-00-000075	CATI - CATI Add	V-63859	WN10-UR-000045
Keyword Filter Exclusive (-) Filter			Inclusive (+) Filter Exclusive (-) Filter	V-63869	WN10-UR-000065
+ / - Rule Title Keyword Filter	V-63365	WN10-00-000080	+ / - Keyword Filter	V-68845	WN10-0R-000065
STIG ID	V-63367	WN10-00-000085	+ CAT I CAT I		
Vulnerability ID	V-63369	WN10-CC-000350		V-68849	WN10-00-000150
Rule ID	V-63371	WN10-00-000090		V-78129	WN10-00-000240
IA Control	V-63373	WN10-00-000095			
	V-63375	WN10-CC-000355			
	V-63377	WN10-00-000100			
	V-63381	WN10-00-000105			
content in table	V-63383	WN10-00-000110			
	V-63385	WN10-00-000115			
Showing	v-63403 v-63405	t of 282	Showing rule 4	out of	25
	V-63409	WN10-AC-000010			
Remove Filter(s) Remove All Filters	V-05409	WINTU-AC-000010	Remove Filter(s) Remove All Filters		

Showing rule 14 out of 282

Showing rule 4 out of 25

😰 DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

Number Number<	Version 1. Polosso 2 Bonshmark Data 14 Nov 2022	Microsoft Windows 11 Security Technical Implementation Guide - Version 1. D	Rule Name +	Rule ID	Vul ID		7 STIGs
Nume Severity: CAT II Classification: Unclass 0 MACK12 22 Sever for Windows Scurity Technical Implementation Guid V32556 V325325682 SRC 0-500018. 0 Apache Sever 24 Windows Steruty Technical Implementation Guid V32576 V325326782. SRC 0-500018. 0 Critic Window Steruty Technical Implementation Guid V32586 V325326882. SRC 0-500018. 0 Critic Window Steruty Technical Implementation Guid V32586 V325326882. SRC 0-500018. 0 Critic Window Steruty Technical Implementation Guid V32586 V325326882. SRC 0-500018. 0 V325868 V325326882. SRC 0-500018. SRC 0-500018. 0 V32586 V325326882. SRC 0-500048. SRC 0-500048. V325868 V325326882. SRC 0-500048. SRC 0-500048. V325868 V325326882. SRC 0-500048.	-						
C AVACHE 2.2 Server for Window Sscurity Technical Implementation Gill AVACHE 2.2 Server for Window Sscurity Technical Implementation Gill V3:3257 SV 2323692 SR 0-5000012, Apache Server 2.4 Windows Strew Stecurity Technical Implementation Gill V3:3257 SV 2323692 SR 0-5000012, Apache Server 2.4 Windows Strew Stecurity Technical Implementation Gill V3:3250 SV 2323692 SR 0-5000012, Apache Server 2.4 Windows Strew 2.4 Windows Strew 2.4 Windows Strew 2.0 Windows Winau Delivery Agent Security Technical Implementation Gill V3:3250 SV 2332692 SR 0-500002, Affacter Current Windows Security Technical Implementation Gill V3:3250 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-50002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3260 SV 2332692 SR 0-500002, V3:3276 SK 0-50002, SR 0-500002, V3:3277 SV 23327692 SR 0-50		_					
ArAche 22 Stryle 10: Windows Security Technical Implementation Gald							
// Apple Server 24 Windows Server 24 Windows Security Technical Implementation Gide // 253258 SV-25325882 SG-05-00004. // 253258 SG-05-00014. // 253268 SG-25-00014. // 253268 SG-05-00014. // 253278 SG-05-000014. // 253278							
• Apache Server 24 Windows Stever 24 Windows Wintual Delixey Agent Security Technical Implementation Current V25325 SV-2532602 SRG-05-00042. Citrix KanDexkop 7 x Windows Vintual Delixey Agent Security Technical Implementation Current Windows Steverity Technical Implementation Guide V25326 SV-2532682. SRG-05-00024. Ref Title: Secure Boot must be enabled on Windows 11 systems. V25326 SV-2532682. SRG-05-00024. Windows 11 System Steverity Technical Implementation Guide V25326 SV-25326682. SRG-05-00024. Windows 11 System Steverity Technical Implementation Guide V25326 SV-25326682. SRG-05-00024. Windows 11 System Steverity Technical Implementation Guide V25326 SV-25326682. SRG-05-00024. Windows 11 System Steverity Technical Implementation Guide V25326 SV-25326682. SRG-05-00014. Windows 11 System Information Syst							
• Under Suffer						he Server 2.4 Windows Server Security Technical Implementation	Apache Server 2.4 Windows
Currux Numa Unitary Agents Security Technical Implementation V-253261 42. SRG-05-00012. V-253264 52. SRG-05-00012. V-253276 52. SRG-05-00012. V-253276 52. SRG-05-00012. V-253277 52. SRG-05-00002. V						he Server 2.4 Windows Site Security Technical Implementation Gu	Apache Server 2.4 Windows
 Chick Aetholeskup / 2X windows security Technical Implementation Guide V 233266 SV 23326782 SRG-05-00048. V 233266 SV 25327862. SRG-05-00048. V 233276 SV 25327782. SRG-05-0009. V 233276 SV 25327682. SRG-05-0009. V 25327682. SRG-05-0009. V 25327682. SRG-05-0009 V 2		Group Title: SRG-OS-000424-GPOS-00188				Virtual Apps and Desktop 7.x Windows Virtual Delivery Agent Se	Citrix Virtual Apps and Deskt
 Deb Postgres Advanced Server v11 on Windows Security Technical Implementation Guide V=252263 V=252264 V=25226742 SRC 05 00048 V=252266 V=25227642 SRC 05 00048 V=25227 V=25227142 SRC 05 00048 V=25227 V=25227422 SRC 05 00091 V=25227 V=25227422 SRC 05 00092 V=252276 V=252274422 SRC 05 00091		Rule Title: Secure Boot must be enabled on Windows 11 systems				XenDesktop 7.x Windows Virtual Delivery Agent Security Technic	Citrix XenDesktop 7.x Windo
 Unstandin Territoria Security Technical Implementation Guide V253264 V253264 V253264 V253264 V253264 V253264 V253264 V253264 V253266 V253266 V25326762 SRG-OS-00048. V253267 V25326782 SRG-OS-00048. V253267 V25326782 SRG-OS-00048. V253267 V25326782 SRG-OS-00048. V25327 V2532762 SRG-OS-00048. V25327 V2532762 SRG-OS-00048. V25327 V25327762 SRG-OS-00048. V25328 V25327762 SRG-OS-00048. V25328 V25327762 SRG-OS-00048. V25328 V253287622 SRG-OS-00048. V25328		Rule The Sectre Boot must be enabled on windows in systems.				Postgres Advanced Server v11 on Windows Security Technical Im	EDB Postgres Advanced Serv
Microsoft Windows 10 Security Technical Implementation Guide V.253265 SV-253266/R2L. SR-05-00008. V.253266 SV-253266/R2L. SR-05-00013 V.253266 SV-253266/R2L. SR-05-00013 V.253266 SV-253266/R2L. SR-05-00013 V.253276 SR-05-00013 V.253276 SR-05-00013 V.253270 SV-253266/R2L. SR-05-00013 V.253276 SR-05-00013 V.253276 SR-05-00013 V.253276 SR-05-00013 V.253276 SR-05-00013 V.253276 SR-05-00013 V.253276 SR-05-00013 V.253277 SV-2532762 SR-05-00013 V.253277 SV-25327762 SR-05-00013 V.253277 SV-25327762 SR-05-00009 V.253277 SV-25327762 SR-05-00009 V.253277 SV-2532762 SR-05-00009 V.253277 SV-2532762 SR-05-00009 V.253277 SV-2532762 SR-05-00009 V.253278 SV-2532762 SR-05-00009 V.253278 SV-2532762 SR-05-00009 V.253278 SV-2532762 SR-05-00009 V.253278 SV-2532762 SR-05-00009						Jle Chrome Current Windows Security Technical Implementation	Google Chrome Current Win
Victoresoft Windows 11 Security Technical Implementation Guide V-253266 SW-253266602 SRG-05-00048. Wicrosoft Windows Server 2012/2012 R2 Domain Controller Security Technical Implementation Subject Techning Subject Technical Implementation Subject Techni	n-based Security and Credential Guard. If Secure Boot					osoft Windows 10 Security Technical Implementation Guide	Microsoft Windows 10 Secur
Mucksoft Windows server 0/12/2012 R2 bolinain Collodier Security V-253267 SV-25326782 SRG-OS-00013 For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshe V-253268 SV-253266882 SRG-OS-00013 For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshe V-253270 SV-25327682 SRG-OS-00031 For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshe Muck match: All Any V-253270 SV-25327682 SRG-OS-00031 For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshe * /- Keyword Add V-253270 SV-25327682 SRG-OS-00031 Fix Text: Enable Secure Boot in the system firmware. V-253275 SV-25327682 SRG-OS-000031 V-253275 SV-25327682 SRG-OS-000031 Fix Text: Enable Secure Boot in the system implements cryptographic mechanisms to prevent unauth and/or detect changes to information during transmission unless otherwise protected by organization safeguards V-253276 SV-25327682 SRG-OS-00009 V-253276 SV-25327682 SRG-OS-00009 NIST SP 800-53 Revision 4 :: SC-8 (1) V-253286 SV-25328682						osoft Windows 11 Security Technical Implementation Guide	✓ Microsoft Windows 11 Secur
Image: Solution in table V-253268 SV-253269482 SRG-05-0004 For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshe Image: V-253269 SV-253269482 SRG-05-00031 V-25327 SV-25327042 SRG-05-00048 V-25327 SV-25327148 SRG-05-00031 V-25327 V-25327 SV-25327148 SRG-05-00048 V-25327 SV-25327148 SRG-05-00048 V-25327 SV-25327148 SRG-05-00031 V-25327 SRG-05-00048 V-25327 SRG-05-00048 V-25327 SRG-05-00048 V-25328 SRG-05-00048 V-25328		Check Text : Verify the system firmware is configured for Secure Boot.	SRG-OS-00048	SV-253266r82	V-253266	osoft Windows Server 2012/2012 R2 Domain Controller Security T	Microsoft Windows Server 20
Profile No Profile V-253268 SV-25326882 SRG-05-00046 Num "System Information". ✓ Filter Panel V-253269 SV-25327082 SRG-05-00048 Num "System Information". Under "System Summary", if "Secure Boot State" does not display "On", this is a finding. ✓ Liter filter keyword Add V-253271 SV-253271482 SRG-05-00048 Yufer "System Summary", if "Secure Boot State" does not display "On", this is a finding. V-253271 SV-253271482 SRG-05-00048 Yufer "System Summary", if "Secure Boot State" does not display "On", this is a finding. V-253273 SV-253271482 SRG-05-0009 Yufer "System Summary", if "Secure Boot State" does not display "On", this is a finding. V-253274 SV-253271482 SRG-05-0009 Yufer "System Summary", if "Secure Boot State" does not display "On", this is a finding. V-253275 SV-253277682 SRG-05-0009 Yufer "System Summary", if "Secure Boot State" does not display "On", this is a finding. V-253276 SV-253277682 SRG-05-0009 Yufer System Summary", if "Secure Boot State" does not display "On", this is a finding. V-253276 SV-253276782 SRG-05-0009 Yufer System Summary", if "Secure Boot State" does not display "O	ance is deleted or refreshed upon logoff, this is NA.	For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted	SRG-OS-00013	SV-253267r82	V-253267	· · · · · · · · · · · · · · · · · · ·	
Filter Panel V-253270 SV-25327082 SRG-OS-00048 V-253271 SV-25327182 SRG-OS-00048 V-253271 SV-253273782 SRG-OS-00048 V-253271 SV-253273782 SRG-OS-00009 V-253271 SV-25327782 SRG-OS-00009 V-253275 SV-253276782 SRG-OS-00009 V-253275 SV-253277782 SRG-OS-00009 V-253275 SV-253277782 SRG-OS-00009 V-253275 SV-253277782 SRG-OS-00009 V-253275 SV-253277782 SRG-OS-00009 V-253285 SRG-O		· · · · · · · · · · · · · · · · · · ·	SRG-OS-00046	SV-253268r82	V-253268	Profile: No Profile 🔹	Profile: No Pro
Must match: All Any		Run "System Information".	SRG-OS-00031	SV-253269r82	V-253269		
Keyword Add V-253272 SKG-05-00048 • /- Keyword Filter Scdusive (-) Filter SKG-05-0007	his is a finding.	Under "System Summary", if "Secure Boot State" does not display "On", this is a finding	SRG-OS-00048	SV-253270r82	V-253270	A	
No content in table V253278 SRG 05 00009 V253276 SV25327182 SRG 05 00007 SRG 05 00007 V25327 SV25327182 SRG 05 00007 SRG 05 00007 V25327 SV25327182 SRG 05 00007 SRG 05 00007 V25327 SV25327182 SRG 05 00009 SRG 05 0009 V25327 SV25327182 SRG 05 0009 SRG 05 0009 V25328 SV25327182 SRG 05 00048 SRG 05 00048 V25328 SV25328182 SRG 05 00048 SRG 05 00048 V25328 SV25328182			SRG-OS-00031	SV-253271r82	V-253271	Must match: All Any	
+/- Keyword Filter V-253273 SV-253273782 SRG-0S-00007 References V-253274 SV-253274r84 SRG-0S-000031 V.253275 SV-253274r84 SRG-0S-000031 CCI: CCI-002421: The information system implements cryptographic mechanisms to prevent unauth and/or detect changes to information during transmission unless otherwise protected by organization and/or detect changes to information during transmission unless otherwise protected by organization v-253276 SV-253277682 SRG-0S-00009 NIST SP 800-53 Revision 4 :: SC-8 (1) No content in table V-253286 SV-253287682 SRG-0S-00048 NIST SP 800-53 Revision 4 :: SC-8 (1) V-253285 SV-253287682 SRG-0S-00048 NIST SP 800-53 Revision 4 :: SC-8 (1) V-253286 SV-253281682 SRG-0S-00048 NIST SP 800-53 Revision 4 :: SC-8 (1)		Fix Text : Enable Secure Boot in the system firmware.	SRG-OS-00048	SV-253272r82	V-253272		-
V-253274 SK-253274r34 SKG-OS-00031 V-253275 SV-253275r32 SKG-OS-00009 V-253276 SV-253276r32 SKG-OS-00009 V-253277 SV-253277r62 SKG-OS-00009 V-253277 SV-253277r82 SKG-OS-00009 V-253277 SV-253277r82 SKG-OS-00009 V-253278 SV-253277r82 SKG-OS-00009 V-253278 SV-253277r82 SKG-OS-00009 V-253280 SV-253279r82 SKG-OS-00009 V-253281 SV-253281r82 SKG-OS-00048 V-253282 SV-253281r82 SKG-OS-00048 V-253281 SV-253281r82 SKG-OS-00048 V-253282 SV-253281r82 SKG-OS-00048 V-253282 SV-253281r82 SKG-OS-00048 V-253282 SV-253281r82 SKG-OS-00048 V-253282 SV-253281r82 SKG-OS-00048 V-253284 SV-253281r82 SKG-OS-00048 V-253285 SV-25328r62 SKG-OS-00048 V-253286 SV-25328r62 SKG-OS-0009		References	SRG-OS-00007	SV-253273r82	V-253273		
V-253275 SV-253275782 SRG-OS-00009 V-253276 SV-253276782 SRG-OS-00009 V-253277 SV-253276782 SRG-OS-00009 V-253277 SV-253277782 SRG-OS-00009 V-253277 SV-253277782 SRG-OS-00009 V-253278 SV-25327782 SRG-OS-00009 V-253278 SV-25327782 SRG-OS-00009 V-253279 SV-25327782 SRG-OS-00009 V-253279 SV-25327782 SRG-OS-00009 V-253280 SV-253279782 SRG-OS-00009 V-253280 SV-253280782 SRG-OS-00048 V-253281 SV-253280782 SRG-OS-00048 V-253282 SV-253280782 SRG-OS-00048 V-253282 SV-253280782 SRG-OS-00048 V-253283 SV-253280782 SRG-OS-00048 V-253284 SV-253280782 SRG-OS-00048 V-253284 SV-253286782 SRG-OS-00048 V-253286 SV-253286782 SRG-OS-00048 V-253286 </td <td>hanisms to provent upouthorized disclosure of informa</td> <td>CCI, CCI, 002421. The information system implements sportagraphic machanisms to pro</td> <td>SRG-OS-00031</td> <td>SV-253274r84</td> <td>V-253274</td> <td>+/- Keyword Filter</td> <td>+/-</td>	hanisms to provent upouthorized disclosure of informa	CCI , CCI, 002421. The information system implements sportagraphic machanisms to pro	SRG-OS-00031	SV-253274r84	V-253274	+/- Keyword Filter	+/-
No content in table V-253277 SV-253277r82 SRG-OS-00009 V-253270 SV-25327882 SRG-OS-00009 V-253270 SV-25327982 SRG-OS-00009 V-253270 SV-25327982 SRG-OS-00009 V-253280 SV-253280r82 SRG-OS-00009 V-253281 SV-253280782 SRG-OS-00048 V-253282 SV-253282r82 SRG-OS-00048 V-253282 SV-253282r82 SRG-OS-00048 V-253283 SV-25328872 SRG-OS-00048 V-253284 SV-253288782 SRG-OS-00048 V-253284 SV-253288782 SRG-OS-00048 V-253284 SV-253288782 SRG-OS-00043 V-253286 SV-253288782 SRG-OS-00043 V-253286 SV-253286782 SRG-OS-00043 V-253286 SV-253286782 SRG-OS-00009 V-253286 SV-253286782 SRG-OS-00009	•		SRG-OS-00009	SV-253275r82	V-253275		
V-253277 SV-25327782 SKG-OS-00009 V-253278 SV-25327882 SRG-OS-00009 V-253279 SV-25327982 SRG-OS-00009 V-253280 SV-253280782 SRG-OS-00048 V-253281 SV-253281782 SRG-OS-00048 V-253282 SV-253281782 SRG-OS-00048 V-253283 SV-253282782 SRG-OS-00048 V-253283 SV-253281782 SRG-OS-00048 V-253283 SV-253283782 SRG-OS-00048 V-253284 SV-253283782 SRG-OS-00043 V-253284 SV-253285782 SRG-OS-00043 V-253284 SV-253285782 SRG-OS-00043 V-253284 SV-253285782 SRG-OS-00043 V-253286 SV-253286782 SRG-OS-00043 V-253286 SV-253286782 SRG-OS-0009		5	SRG-OS-00009	SV-253276r82	V-253276		
No content in table 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-253282 SV-253283r82 SRG-OS-00048 V-253283 SV-253283r82 SRG-OS-00048 V-253283 SV-253283r82 SRG-OS-00043 V-253284 SV-253283r82 SRG-OS-00043 V-253284 SV-253283r82 SRG-OS-00043 V-253285 SV-253285r82 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009		NIST SP 800-53 Revision 4 :: SC-8 (1)	SRG-OS-00009	SV-253277r82	V-253277		
No content in table V-253280 SV-253280782. SRG-OS-00048 V-253281 SV-253281782. SRG-OS-00048 V-253282 SV-253282782. SRG-OS-00048 V-253283 SV-253283782. SRG-OS-00048 V-253283 SV-253283782. SRG-OS-00043 V-253284 SV-253284782. SRG-OS-00043 V-253284 SV-253284782. SRG-OS-00043 V-253285 SV-253285782. SRG-OS-00043 V-253285 SV-253285782. SRG-OS-00043 V-253286 SV-253285782. SRG-OS-00043 V-253286 SV-253286782 SRG-OS-00043			SRG-OS-00009	SV-253278r82	V-253278		
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-253284 SV-253284r82 SRG-OS-00043 V-253284 SV-253284r82 SRG-OS-00043 V-253284 SV-253284r82 SRG-OS-00043 V-253285 SV-253285r82 SRG-OS-0009 V-253286 SV-253286r82 SRG-OS-0009			SRG-OS-00009	SV-253279r82	V-253279		
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			SRG-OS-00048	SV-253280r82	V-253280	No content in table	No (
V-253283 SV-253283r82 SRG-OS-00043 V-253284 SV-253284r82 SRG-OS-00043 V-253285 SV-253285r82 SRG-OS-0009 V-253286 SV-253286r82 SRG-OS-0009			SRG-OS-00048	SV-253281r82	V-253281		
V-253284 SV-253284r82 SRG-OS-00043 V-253285 SV-253285r82 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009			SRG-OS-00048	SV-253282r82	V-253282		
V-253285 SV-253285r82 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009			SRG-OS-00043	SV-253283r82	V-253283		
V-253285 SV-253285r82 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009			SRG-OS-00043	SV-253284r82	V-253284		
V-253286 SV-253286r82 SRG-OS-00009							
Showing rule 4 out of 253			~			Remove Filter(s) Remove All Filters	Remove Filter

Group Title: SRG-OS-000424-GPOS-00188

Rule Title: Secure Boot must be enabled on Windows 11 systems.

Discussion: Secure Boot is a standard that ensures systems boot only to a trusted operating system. Secure Boot is required to support additional security features in Windows 11, including virtualization-based Security and Credential Guard. If Secure Boot is turned off, these security features will not function.

Check Text: Ver

For virtual deskt

Run "System Inf

Under "System

Fix Text: Enable

CCI: CCI-002421 and/or detect ch safeguards.

NIST SP 800-53



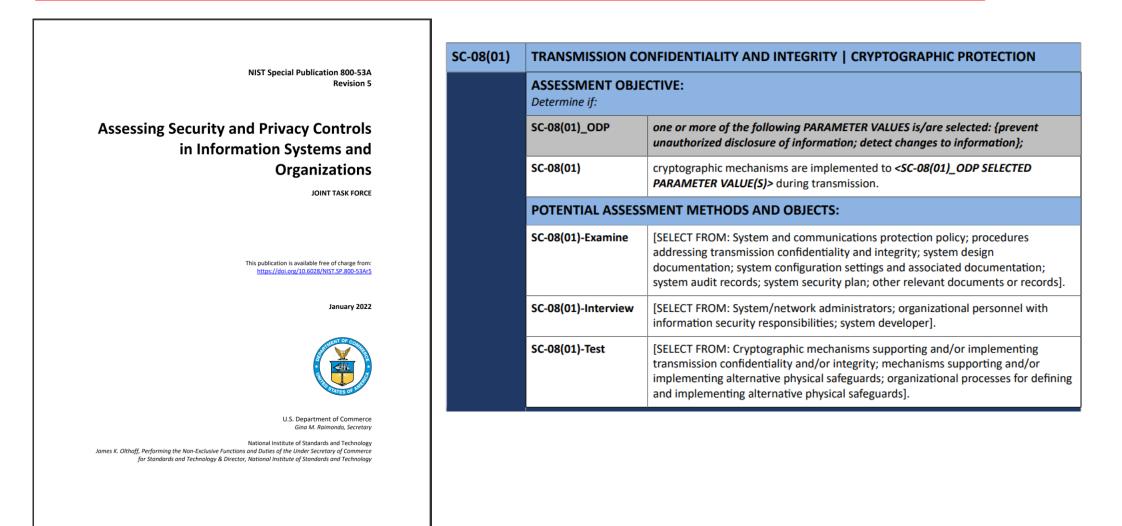
- 🗆 🗙

Verify the system firmware is configured for Secure Boot.		Value
		Microsoft Windows 11 Pro
ktop implementations (VDIs) where the virtual desktop instance is deleted or refreshed upon logoff, this		10.0.22621 Build 22621
	on	Not Available
nformation".		Microsoft Corporation
		MIS-DLANTER-X1E
n Summary", if "Secure Boot State" does not display "On", this is a finding.	er	LENOVO
· · · · · · · · · · · · · · · · · · ·		
le Secure Boot in the system firmware.		x64-based PC
be secure boot in the system innivate.		LENOVO_MT_20Y5_BU_Think_FM_ThinkPad X1 Extreme Gen 4i 11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 2304 Mhz, 8 Core(s), 16 Log
References		LENOVO N40ET37W (1.19), 8/26/2022
		3.2
21: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of	of information ler Ve	/ersion 1.16
changes to information during transmission unless otherwise protected by organization-defined alterna		UEFI
, - <u>, - , - , - , - , - , - , - , - , -</u>	cturer	er LENOVO
3 Revision 4 :: SC-8 (1)		20Y5007QUS
		SDK0T76530 WIN
	Platform Role	Mobile
System information app	Secure Boot State	Off +
y system mornation app	PCR7 Configuration	Elevation equired to View
	Windows Directory	C:\WINDOWS
	System Directory	C:\WINDOWS\system32
	Boot Device	\Device\HarddiskVolume1
	Locale	United States
	Hardware Abstraction La	
	User Name Time Zone	MIS-DLanter-XTE\David Lanter
	Installed Physical Memo	Eastern Daylight Time
	Total Physical Memory	31.7 GB
	Available Physical Memo	
	Total Virtual Memory	33.7 GB
	Available Virtual Memor	
	Page File Space	2.00 GB
	Page File	C:\pagefile.sys
	Kernel DMA Protection	
	Virtualization-based sec	curity Running
Find <u>w</u> hat:		Find Close Find
Search selected category only	Search c	category names only
snowing rule 4 out o	a) (49)5)	
All all a second and a second as		
system Information 🛛 🔲 💽 🚺 🚞 🚭 😰 💷	M	

References

CCI: CCI-002421: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards.

NIST SP 800-53 Revision 4 :: SC-8 (1)



😵 DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

Winds Interstent Marchaet	▼ STIGs	Vul ID	Rule ID	Rule Name			
Water Value Value <td< th=""><th></th><th></th><th></th><th></th><th></th></td<>							
Model 22 Sever for Window Security Technical implementation Gal V32256 9V 232562 956 05 00042 Model 22 Sever for Window Security Technical implementation Gal V33257 9V 3232662 956 05 00042 Model Security Technical implementation Gal V33257 9V 3232662 956 05 00042 V33257 Model Security Technical implementation Gal V33257 9V 3232662 956 05 00042 V33257 V3325 Sever 210 Window Structury Technical implementation Gal V33257 9V 3232668 956 05 00042 V3325 Sever 210 Window Structury Technical implementation Gal V33257 9V 3232668 956 05 00042 V3326 Sever 210 Window Structury Technical implementation Gal V332586 9V 2322668 956 05 00042 V3326 Sever 2102 Window Y11 Window Structury Technical implementation Gal 90 V3232688 95 V3232688 95 V3232688 V3326 Sever 2102 Window Y11 Window Structury Technical implementation Gal 90 V323268 95 V3232688 95 V3232688 V3326 Sever 2102 Window Y11 Window Structury Technical implementation Gal 90 V323268 95 V3232688 95 V3232688 95 V323268 95 V323268 95 V323268 95 V323268 95 V3232688 95 V323268 95 V32							
Visites Normality					Severity. CAT II Classification. Onclass		
were files were fi	APACHE 2.2 Server for Windows Security Technical Implementation Gu						
Partial Server 24 Windows Starver	APACHE 2.2 Site for Windows Security Technical Implementation Guid						
 Prove Time Towe All files Prove	Apache Server 2.4 Windows Server Security Technical Implementation						
Unit witching high and books by LA Wildow Statudies of Wildow Stat	Apache Server 2.4 Windows Site Security Technical Implementation Gu						
 	Citrix Virtual Apps and Desktop 7.x Windows Virtual Delivery Agent Se				Group Title: SRG-OS-000404-GPOS-00183		
Image: Construction of Security Technical Implementation Guide V-25226 SV-25226682 SG CO-500048. V-252268 SV-25226682 SG CO-500048. V-252268 V-252268 V-252268 V-252268 SV-25226862 SG CO-500048. V-252268 V-252268 V-252268 V-252268 V-252268 SV-25226862 SG CO-500048. V-25226 V-252268 V-252278 V-252278 <td>Citrix XenDesktop 7.x Windows Virtual Delivery Agent Security Technic</td> <td></td> <td></td> <td></td> <td>Pule Title: Windows 11 information systems must use Pitlesker to apprent all disks to protect the confidentiality and integrity of</td>	Citrix XenDesktop 7.x Windows Virtual Delivery Agent Security Technic				Pule Title: Windows 11 information systems must use Pitlesker to apprent all disks to protect the confidentiality and integrity of		
 Discussion: If data at rest is unencrysted, it is vulnerable to disclosure. Even if the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at a comparison of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at the system entor of the operating system enforces permissions on d and exercise at the system entor of the operating system entor or at the entore the system entor of the operating system entor or and exercise at the system entor or and exercise at the system entor or and exercise at the system entore permission at the exercise at the system entores permissio	EDB Postgres Advanced Server v11 on Windows Security Technical Im						
 Microadi Windows 1 Security Technical impermitation suggest Microadi Windows 1 Security Technical impermitation suggest Microadi Windows Server 2012/2012 R2 Domain Controller Security Prefile Prefile Prefile Prefile Prefile Prefile Microadi Windows 1 Security V-23286 V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23286/R2_SRG-05:00046, V-23287/R2_SRG-05:00046, V-23288/R2_SRG-05:00046, V-23288/R2_SRG-05:00046, V-23288/R2_SRG-05:00046, V-23288/R2_SRG-05:00046, V-23288/R2_SRG-05:00046, V-23288/R2_SRG-05:00046,<!--</td--><td>Google Chrome Current Windows Security Technical Implementation</td><td></td><td></td><td></td><td></td>	Google Chrome Current Windows Security Technical Implementation						
V Encrosoft Windows 11 Security Technical Implementation Guide V-253266 SR-25326882. SRG-05-00012. SRG-05-00012. V Postle No Postle V-253266 SR-25326882. SRG-05-00012. SRG-05-00012. V 253267 V-25326882. SRG-05-00012. SRG-05-00012. SRG-05-00012. V 253267 V-25326882. SRG-05-00012. SRG-05-00012. SRG-05-00012. V 253267 V-25326882. SRG-05-00012. SRG-05-00012. SRG-05-00012. V 253267 V-25327082. SRG-05-00012. SRG-05-00012. SRG-05-00012. V 253271 V-25327182. SRG-05-00014. V-253271 V-25327182. SRG-05-00014. If full disk encryption using BitLocker is not implemented. this is a finding. V 253271 V-25327182. SRG-05-00014. V-253271. V-25327182. SRG-05-00014. If full disk encryption using BitLocker is not implemented. This is a finding. V 253271 V-25327182. SRG-05-00014. V-253276. V-2532782. SRG-05-00024. If the operating system drive and any fixed data drives. Operating in the origination requirements (NVII-00-000022). If the operating system drive and any fixed data drives. Operating s	Microsoft Windows 10 Security Technical Implementation Guide	V-253264					
Vestion Profile Vestig SVestig	Microsoft Windows 11 Security Technical Implementation Guide	V-253265	SV-253265r82	SRG-OS-00008			
V25286 V252866 V25287 V25287 V25287 V25287 V252877	Microsoft Windows Server 2012/2012 R2 Domain Controller Security T	V-253266	SV-253266r82	SRG-OS-00048			
Vestage Vestage SV-253269/R2. SRG-05-0004 Nor AND Implementations with no deskup instance's detected of refreshed upon logicit, inits is NA. Vestage SV-253270 SV-253270R2. SRG-05-0004 Vestage Nor AND Implementations with no deskup instance's detected of refreshed upon logicit, inits is NA. Vestage SV-253270 SV-253270R2. SRG-05-0004 Vestage Vestage Vestage Vestage SV-253270 SV-253270R2. SRG-05-0003 Vestage Vestage Vestage Vestage SV-253271 SV-253270R2 SRG-05-0003 Vestage Vestage Vestage Vestage SV-253270R2 SRG-05-0003 Vestage Vestage Vestage Vestage Vestage SV-253270R2 SRG-05-0000 Vestage Network Vestage V		V-253267	SV-253267r82	SRG-OS-00013	Check Text: Verify all Windows 11 information systems (including SIPRNet) employ BitLocker for full disk encryption.		
V Effer Panel V-253270 SV-253270/R2. SR-C-OS-00048 If full disk encryption using BitLocker is not implemented, this is a finding. V-253271 SV-253271/R2 SR-G-OS-00048 Verify BitLocker is not implemented, this is a finding. V-253271 SV-253271/R2 SR-G-OS-00048 Verify BitLocker is not implemented, this is a finding. V-253271 SV-253271/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253275 SV-253271/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253275 SV-253271/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253275 SV-25327/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253275 SV-25327/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253276 SV-25327/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253286 SV-25327/R2 SR-GOS-00048 Verify BitLocker is not implemented, this is a finding. V-253286 SV-25328/R2 SR-GOS-00048 Note natternet encryption any fixed data drives nor any fixed data drives	Profile: No Profile 👻	V-253268	SV-253268r82	SRG-OS-00046	For virtual desktop implementations (VDIs) in which the virtual desktop instance is deleted or refreshed upon logoff, this is NA.		
Must match: All All V-253271 SV-253271R32 SRG-OS-0004 V-253272 SV-25327R42 SRG-OS-0004 V-253273 SV-25327R42 SRG-OS-0004 V-253273 SV-25327R42 SRG-OS-0004 V-253273 SV-25327R42 SRG-OS-0004 V-253273 SV-25327R42 SRG-OS-0004 V-253274 SV-25327R42 SRG-OS-0004 V-253275 SV-25327R42 SRG-OS-0004 V-253276 SV-25327R42 SRG-OS-0009 V-25328 SV-25328R42 SRG-OS-0009		V-253269	SV-253269r82	SRG-OS-00031	For AVD implementations with no data at rest, this is NA.		
Must match: All Aug Keyword Inter filter Keyword Add V-25327 SV-253271/82 SRG-05-00048 V-25327 SV-25327382 SRG-05-00048 V-25327 SV-25327382 SRG-05-00031 V-25327 SV-25327382	▼ Filter Panel	V-253270	SV-253270r82	SRG-OS-00048	If full disk encryption using BitLocker is not implemented, this is a finding.		
• Inclusive (1) Filter Exclusive (2) Filter + /- Keyword Filter V-253273 SV-25327782 SRG-OS-00007 V-253275 SV-25327782 SRG-OS-00009 V-253276 SV-25327782 SRG-OS-00009 V-253276 SV-25327782 SRG-OS-00009 V-253276 SV-25327782 SRG-OS-00009 V-253277 SV-25327782 SRG-OS-00009 V-253276 SV-25327782 SRG-OS-00009 V-253276 SV-25327782 SRG-OS-00009 V-253277 SV-25327782 SRG-OS-00009 V-253277 SV-25327782 SRG-OS-00009 V-253277 SV-25327782 SRG-OS-0009 V-253281 SV-2532782 SRG-OS-00048 V-253281 SV-25328782 SRG-OS-00048 V-253281 SV-25328782 SRG-OS-00048 V-253282 SV-25328782 SRG-OS-00048 V-253283 SV-25328782 SRG-OS-00048 V-253284 SV-25328782 SRG-OS-00048 V-253284 SV-25328782 SRG-OS	Must match: All Any	V-253271	SV-253271r82	SRG-OS-00031			
+ / - Keyword Filter V-232/73 SV-232/7482 SKG-05-00007 Open "BitLocker Drive Encryption" from the Control Panel. V-253274 SV-25327462 SKG-05-00009 If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding. V-253275 SV-25327762 SKG-05-00009 V-253276 SKG-05-00009 V-253276 SV-25327762 SKG-05-00009 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption an satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032). V-253276 SV-25327762 SKG-05-00009 Note: An alternate encryption and linformation systems (including SIPRNet) using BitLocker. V-253271 SV-25327762 SKG-05-00009 Y-253276 SKG-05-00009 V-253270 SV-25327762 SKG-05-00009 Y-253276 SKG-05-00009 V-253281 SV-25328762 SKG-05-00009 Y-253276 SKG-05-00009 V-253282 SV-25328762 SKG-05-00009 Y-253286 SKG-05-00009 V-253282 SV-25328762 SKG-05-00009 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encr		V-253272	SV-253272r82	SRG-OS-00048	Verify BitLocker is turned on for the operating system drive and any fixed data drives.		
+/- Keyword Filter V-253276 SV-2532748 SRG-OS-0003 If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding. V-253276 SV-2532768 SRG-OS-0009 SRG-OS-0009 V-253276 SV-2532768		V-253273	SV-253273r82	SRG-OS-00007	Open "BitLocker Drive Encryption" from the Control Panel.		
 V-25227 SV-25327582. SRG-OS-0009 V-25327 SV-25327582. SRG-OS-0009 V-25327 SV-25327782. SRG-OS-0009 V-25327 SV-25327782. SRG-OS-0009 V-25327 SV-25327882. SRG-OS-0009 V-25328 SV-25328782. SRG-OS-0009 V-25328 SV-25328782. SRG-OS-0009 V-25328 SV-25328782. SRG-OS-0009 V-25328 SV-25328782. SRG-OS-0009 V-25328 SV-253281782. SRG-OS-00048 V-25328 SV-253281782. SRG-OS-00049 V-25328 SV-253281782. SRG-OS-00049 V-25328 SV-253281782. SRG-OS-00049 V-25328 SV-253281782. SRG-OS-00049 V-25328 SV-253281782	+ / - Keyword Filter	V-253274	SV-253274r84	SRG-OS-00031			
No content in table V-253277 SV-25327782 SRG-0S-0009		V-253275	SV-253275r82	SRG-OS-00009	If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.		
No content in table V-25327 SV-253278r2 SRG-OS-00009 V-253280 SV-253279r2 SRG-OS-00009 Fix Text: Enable full disk encryption on all information systems (including SIPRNet) using BitLocker. V-253280 SV-253280r2 SRG-OS-00009 Fix Text: Enable full disk encryption on all information systems (including SIPRNet) using BitLocker. V-253280 SV-253280r2 SRG-OS-00048 Fix Text: Enable full disk encryption and linformation systems (including SIPRNet) using BitLocker. V-253281 SV-253281r82		V-253276	SV-253276r82	SRG-OS-00009	Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and		
No content in table V-253279 SV-253279782 SRG-OS-00009 BitLocker, included in Windows, can be enabled in the Control Panel under "BitLocker Drive Encryption" as well as other management tools. V-253280 SV-25328182 SRG-OS-00048 BitLocker, included in Windows, can be enabled in the Control Panel under "BitLocker Drive Encryption" as well as other management tools. V-253281 SV-25328182 SRG-OS-00048 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and WN11-00-000031. V-253282 SV-253281782 SRG-OS-00048 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and WN11-00-000032. V-253284 SV-253285782 SRG-OS-00048 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253285 SV-253285782 SRG-OS-00009 CC: CCI-002475: The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components. Remove Filter(s) Remove All Filters SV-253286782		V-253277	SV-253277r82	SRG-OS-00009	satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032).		
No content in table V-253279 SV-25327962 SRG-OS-0009		V-253278	SV-253278r82	SRG-OS-00009	Fix Text: Enable full disk encryption on all information systems (including SIPRNet) using Bitl ocker		
No content in table V-253280 SV-253280782 SRG-OS-00048 management tools. V-253281 SV-253281782 SRG-OS-00048 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and wh11-00-000031 and Wh11-00-000032 V-253283 SV-253283782 SRG-OS-00048 Note: An alternate encryption application requirements (Wh11-00-000031 and Wh11-00-000032). V-253284 SV-253286782 SRG-OS-00048 Note: An alternate encryption application requirements (Wh11-00-000031 and Wh11-00-000032). V-253285 SV-253285782 SRG-OS-00048 Note: An alternate encryption application requirements (Wh11-00-000031 and Wh11-00-000032). V-253286 SV-253285782 SRG-OS-00048 Note: An alternate encryption application requirements (Wh11-00-000031 and Wh11-00-000032). V-253285 SV-253285782 SRG-OS-00049 Note: An alternate encryption application requirements (Wh11-00-000031 and Wh11-00-000032). V-253286 SV-253286782 SRG-OS-00049 Note: An alternate encryption application requirements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components. V-253286 SV-253286782 SRG-OS-00009		V-253279	SV-253279r82	SRG-OS-00009			
V-253281 SV-253281r82 SRG-OS-00048 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and WN11-00-000032 V-253283 SV-253283r82 SRG-OS-00048 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and WN11-00-000032 V-253284 SV-253284r82 SRG-OS-00043 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253285 SV-253284r82 SRG-OS-00043 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253286 SV-253286r82 SRG-OS-00043 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253286 SV-253286r82 SRG-OS-00009 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. V-253286 SV-253286r82 SRG-OS-00009 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009 SRG-OS-00009 V-253286 SV-253286r82 SRG-OS-00009 SRG-OS-0009 V-253286 SV-253286r82 SRG-OS-0009	No content in table	V-253280	SV-253280r82	SRG-OS-00048			
V-253282 SV-253282r82 SRG-OS-00048 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and VN11-00-000032). V-253283 SV-253283r82 SRG-OS-00043 Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and VN11-00-000032). V-253284 SV-253283r82 SRG-OS-00043 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253285 SV-253285r82 SRG-OS-00043 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253285 SV-253285r82 SRG-OS-00043 Note: An alternate encryption application requirements (WN11-00-000031 and WN11-00-000032). V-253286 SV-253285r82 SRG-OS-00009 Note: An alternate encryption application requirements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information at re		V-253281	SV-253281r82	SRG-OS-00048	management tools.		
V-253283 SV-253283r82 SRG-OS-00043 SRd-OS-00043 References V-253284 SV-253285r82 SRG-OS-00043 Cl: CCI-002475: The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components. Remove Filter(s) Remove All Filters SV-253286r82 SRG-OS-0009 NIST SP 800-53 Revision 4 :: SC-28 (1)		V-253282 SV-253282r82 SRG-QS-00048 Note: An alternate encryption application may be use		Note: An alternate encryption application may be used in lieu of BitLocker providing it is configured for full disk encryption and			
V-253284 SV-253284r82 SRG-OS-00043 References V-253285 SV-253285r82 SRG-OS-00009 CI:					satisfies the pre-boot authentication requirements (WN11-00-000031 and WN11-00-000032).		
Remove Filter(s) Remove All Filters SV-253285r82 SRG-OS-00009 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)					References		
Remove Filter(s) Remove All Filters V-253286 SV-253286r82 SRG-OS-00009 V-253286r82 SRG-OS-0009 V-253286r82 SRG-OS-009 V-253286r82 SRG-					CCL CCL 002475. The information material mathematic mathematic mathematic and a mathematical state of the state		
Remove Filter(s) Remove All Filters NIST SP 800-53 Revision 4 :: SC-28 (1)							
	Remove Filter(s) Remove All Filters	V					

Group Title: WN10-00-000030

Fig

Bit

C

CC de

NI

CC

de

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.

anarating sustam drive or any fived data drives have "Turn on Pitlocker" this is a finding

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

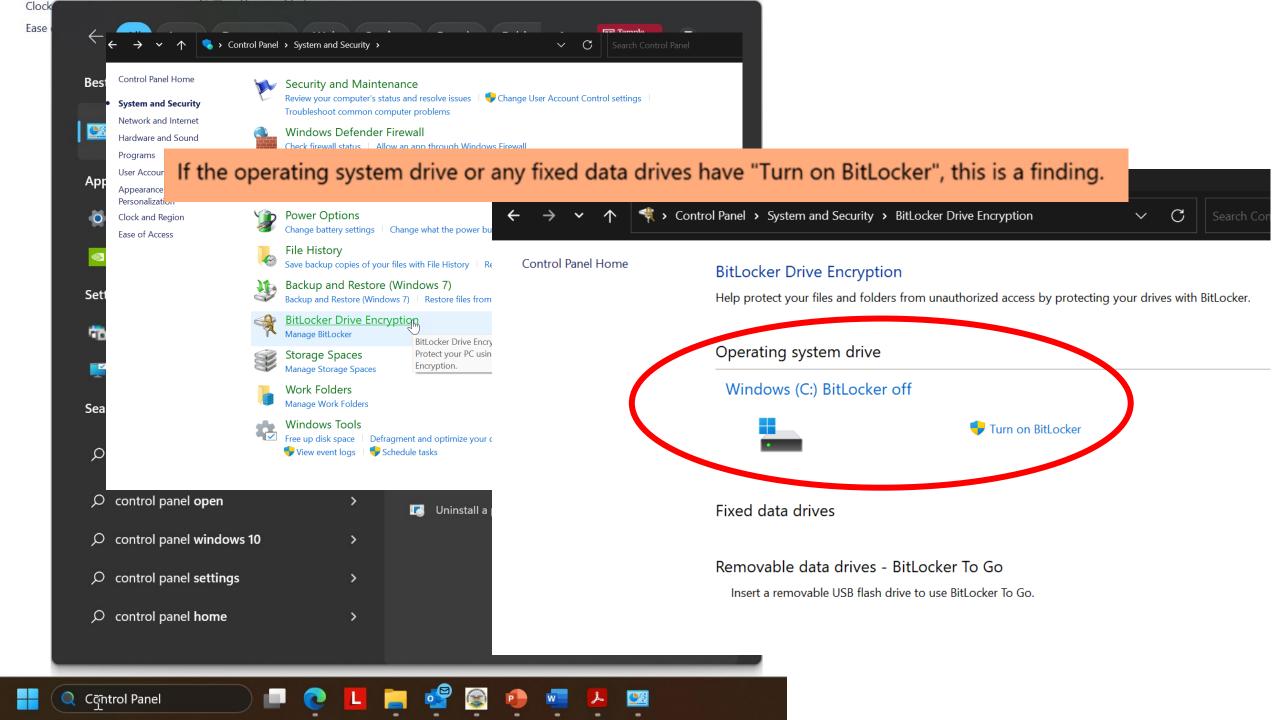
If full disk encryption is not implemented, this is a finding.

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.



Agenda

- ✓ Risk Management Framework A quick review...
- ✓ Implementing controls Host hardening...
 ✓ Security configuration checklist (with STIG Viewer)
- SCAP Security Content Automation Protocol
- System Security Plan's Appendix 1
 - Select 1 Technical control family to fill out for your information system
- System Security Plan's System Information
 - Information System Type
- Team Project SSP draft development...

Agenda

- ✓ Risk Management Framework A quick review...
- ✓ Implementing controls Host hardening...
 ✓ Security configuration checklist (w/DISA STIG Viewer)
- SCAP Security Content Automation Protocol
- System Security Plan's Appendix 1
 - Select 1 Technical control family to fill out for your information system
- Team Project SSP draft development...

SCAP (Security Content Automation Protocol) pronounced "ess-cap"

Purpose: Used for continuously monitoring deployed computer systems and applications for detectable vulnerabilities and assure they incorporate security upgrades to software ("patches") and deploy updates to configurations

SCAP based on a number of open standards, widely used to enumerate software flaws and configuration issues related to security

- The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP
 - Vendors can get their computer system configuration scanner product validated against SCAP, demonstrating that it will interoperate with other scanners and express the scan results in a standardized way
- Validated tools for automating collection of assessment objects used in Examine, Inspect and Test activities

https://en.wikipedia.org/wiki/Security_Content_Automation_Protocol

Examine: SCAP (Security Content Automation Protocol) validated tools may be used to automate collection of assessment objects

- Common SCAP uses
 - Security configuration verification
 - Compare settings in a checklist to a system's actual configuration
 - Verify configuration before deployment, audit/assess/monitor operational systems
 - Map individual settings to high-level requirements (requirements traceability)
 - Verifying patch installation and identifying missing patches
 - Check systems for signs of compromise
 - Known characteristics of attacks, such as altered files or the presence of a malicious service



Security Content Automation Protocol (SCAP)

SECURITY TECHNICAL Implementation guides (stigs)

DoD Annex for NIAP Protection Profiles

Home *Security Technical Implementation Guides (STIGs) *Security Content Automation Protocol (SCAP)

SCAP 1.3 CONTENT

TITLE	SIZE \$	UPDATED \$
Cisco IOS-XE Router NDM STIG Benchmark - Ver 1, Rel 6	15.35 KB	13 Jan 2023
Cisco IOS-XE Router RTR STIG Benchmark - Ver 1, Rel 2	6.95 KB	21 Oct 2022

SCAP 1.2 CONTENT

TITLE	▲ SIZE	¢	UPDAT
Adobe Acrobat Reader DC Continuous Track STIG Benchmark - Ver 2, Rel 2	10.86 KB		21 Oct 20
Canonical Ubuntu 18.04 LTS STIG Benchmark - Ver 2, Rel 8	62.01 KB		13 Jan 20
Canonical Ubuntu 20.04 LTS STIG Benchmark - Ver 1, Rel 5	61.15 KB		13 Jan 20
Google Chrome STIG Benchmark - Ver 2, Rel 8	24.25 KB		13 Jan 20
Microsoft.NET Framework 4 STIG Benchmark - Ver 2, Rel 2	7.51 KB		13 Jan 20
Microsoft Defender Antivirus STIG Benchmark - Ver 2, Rel 3	23.2 KB		25 May 2
Microsoft Edge STIG Benchmark - Ver 1, Rel 2	1.53 MB		27 Oct 20
Microsoft Internet Explorer 11 STIG Benchmark - Ver 2, Rel 4	66.02 KB		13 Jan 20
Microsoft Windows 10 STIG Benchmark - Ver 2, Rel 7	100.42 KB		13 Jan 20
Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 1	94.76 KB		17 Nov 20

~~

SCAP TOOLS

SCAP Audit Summary

1036177

Options -

0- >

SCAP Audit Summary - Top 25 Linux Compliance Failed Checks

Plugin ID	Name	Severity	Total
1036199	CCE-27239-3::SV-68627r3_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036197	CCE-26875-5::SV-65579r1_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036193	CCE-27283-1::SV-50495r1_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036192	CCE-27283-1::SV-50493r1_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036191	CCE-27081-9::SV-50492r2_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036189	CCE-27626-1::SV-50488r3_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036182	CCE-27119-7::SV-50475r1_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036181	CCE-27254-2::SV-50473r2_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1
1036180	CCE-27515-6::SV-50472r1_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1

Plugin ID Name Severity Total High 1035021 CCE-43078-5::SV-78115r1 rule:Windows 10 STIG 001.007:MAC-1 Classified High 1035018 CCE-42970-4::SV-78109r1_rule:Windows_10_STIG_001.007:MAC-1_Classified 1035012 CCE-43470-4::SV-78091r1_rule:Windows_10_STIG_001.007:MAC-1_Classified High 1034963 CCE-42218-8::SV-77923r2_rule:Windows_10_STIG_001.007:MAC-1_Classified 1034959 High CCE-42218-8::SV-77915r2_rule:Windows_10_STIG_001.007:MAC-1_Classified 1034952 CCE-42187-5::SV-77901r2_rule:Windows_10_STIG_001.007:MAC-1_Classified High

CCE-42073-7::SV-77897r2_rule:Windows_10_STIG_001.007:MAC-1_Classified

SCAP Audit Summary - Top 25 Windows Compliance Failed Checks

CCE-26741-9::SV-5047251_rule:RHEL_6_STIG_001.017:MAC-1_Classified

1034950

SCAP Audit Summary - Top 10 CCE

Last Updated: Less than a minute ago unique identifiers to security-related system configuration issues



High Host Total High Host Total High Celevine Ce

SCAP Compliance Scan Results

	ssg-fedo	ora-ds.xml - SCAP Workbench	×				
File Help							
Title	Guide to the Secure Configura	ation of Fedora					
Customization	(no customization)						
Frofile	Common Profile for General-Purpose Fe	siora Systems	- Custamize				
Target	Local Machine	○ Remote Machine (over 55H)					
• gpgcheck E	nobled in Main Yum Configuration		fail				
gpgcheck E	nabled For All Yum Package Repositories		pass				
► Disable Pre	linking		pass				
. Build and R	est AIDE Database		fail				
 Verify and 0 	Correct File Permissions with RPM		fail				
Verify File F	lashes with RPM		pass				
 Shared Libr 	ary Files Have Restrictive Permissions		pass				
Shared Libr	ary Files Have Root Ownership		pass				
► System Exc	cutables Have Restrictive Permissions		pass				
 System Ext 	cutables Have Root Ownership		fail				
· Direct root	Logins Not Allowed		fail				
► Virtual Con	sole Root Logins Restricted		pasa				
* Serial Port I	Root Logins Restricted		pass				
+ Only Root H	tas UID 0		pass				
L		is (72 results, 72 rules selected)	Support of the local division of the local d				
		Clear Save Results	Show Report				
Processing has b	een finished!						

SCAP: Individual compliance check result for scanned host

Nessus Scans Policies		admin 🔻 🐥
Windows 7 SCAP Scan CURRENT RESULTS: NOVEMBER 11, 2014 10:53:16	Configure	Audit Trail Launch 💌 Export 💌
Scans > Hosts 1 Vulnerabilities 2 Compliance 270 History 1		
FALLED CCE-10103-0: Always prompt client for password upon connection	< >	Reference Information
Description		UPDATED-DATE: 2012-02-24T10:00:00 RULE-ID: xccdf_gov.nist_benchmark_USGCB-
Always prompt client for password upon connection		Windows-
The "Always Prompt Client for Password upon Connection" policy should be set correctly for Terminal Services.		7:xccdf_gov.nist_profile_united_states_government_ configuration_baseline_version_1.2.3.1:xccdf_gov.nis t_rule_always_prompt_for_password_upon_connecti on
Audit File		GENERATED-DATE: 2012-02-24T10:00:00 SCAN-DATE: 2014-11-11T16:53:40
Win7-510-1.2.7.1.zip		OVAL-DEF: oval:gov.nist.usgcb.windowsseven:def:275 CCE: CCE-10103-0
Policy Value		SEVERITY: unknown
xccdf_gov.nist_rule_always_prompt_for_password_upon_connection: PASSED		
Output		

xccdf gov.nist rule always prompt for password upon connection: FAILED

SCAP (Security Content Automation Protocol) validated tools may be used to automate collection of assessment objects

- National Vulnerability Database (NVD): <u>https://nvd.nist.gov/</u>
- NVD SCAP Download: http://nvd.nist.gov/download.cfm
- National Checklist Program (NCP): <u>http://web.nvd.nist.gov/view/ncp/repository</u>
- NIST SP 800-126r3, The Technical Specification for SCAP
- NIST SP 800-70r4, National Checklist Program for IT Products
- More documentation and tools:

https://csrc.nist.gov/projects/security-content-automation-protocol/scap-releases

NIST Special Publication 800-70 Revision 4

National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

Stephen D. Quinn Murugiah Souppaya Melanie Cook Karen Scarfone

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-70r4

COMPUTER SECURITY



DISA STIG Tool

SCAP Tool

File Export Checklist O	ptions Help				C Soc	urityC
STIG Explorer					e sec	unityC
▼ STIGs		Vul ID	Rule Name	.+ Windows 10 Security Technical Implementation Guide :: Release: 12 Benchmark Date: 26 Jan 2018		
cx	Name	+ V-63337	WN10-00-000030	Vuln ID: V-63337 Rule ID: SV-77827r1_rule STIG ID: WN10-00-000030	SCAP A	ludit s
		^ V-63349	WN10-00-000040	Severity: CAT Check Reference: M Classification: Unclass		
Windows Firewall with Advanced Security Security Te		V-63351	WN10-00-000045		SCAP Audit	Summary -
	Controller Security Technical I	V-73811	WN10-00-000046		Plugin ID	Name
	Server Security Technical Imp	V-63353	WN10-00-000050		Plugin ID	Name
	2 Domain Controller Security	V-63361	WN10-00-000070		1003887	CCE-N
	2 Member Server Security Tec	V-63377	WN10-00-000100		10038	CCE-17
	012 R2 Domain Controller Sec	V-68845	WN10-00-000145		10038	CUE-17
	012 R2 Member Server Securi	V-68849	WN10-00-000150		10038	CCE-18
	ecurity Technical Implementat	V-78129	WN10-00-000240		10038	CCE-17
	chnical Implementation Guide	V-63429	WN10-AC-000045	Group Title: WN10-00-000030		000.0
	hnical Implementation Guide	V-63651	WN10-CC-000155	Rule Title: Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.	10038	CCE-177
	Technical Implementation Gu	- V-63667	WN10-CC-000180	Nue little: Mooile systems must encrypt all disks to protect the connidentiality and integrity of all information at rest.	1003881	CCE-15
VMware ESXi Server 5.0 Security Technical Implement Profile: MAC-3_Public *		V-63671	WN10-CC-000185	Discussion: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data		
		V-63673	WN10-CC-000190	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.	10038	CCE-14
 Filter Panel 		V-63325	WN10-CC-000315		10038	CCE-M
		V-63335	WN10-CC-000330	Check Text: Verify mobile systems employ DoD-approved full disk encryption.		
CATI	- CATI Add	V-63347	WN10-CC-000345	If full disk encryption is not implemented, this is a finding.	1003878	CCE-54
+/-	Inclusive (+) Filter Exclusive (-) Filter Keyword Filter	V-63739	WN10-SO-000140	If BitLocker is used, verify it is turned on for the operating system drive and any fixed data drives.	10038	CCE-14
4//-	CAT I CAT I	V-63745	WN10-SO-000145	Open "BitLocker Tovie Encryption" from the Control Panel.		
	GIT	V-63749	WN10-SO-000150	If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.	Lest Updated: 1	I hour ago
		V-63759	WN10-SO-000165	It one operating system unvelor any naed data drives have inter on uncooker, dis is a multing.	SCAP Audit	Summary -
		V-63797	WN10-SO-000195	Fix Text: Install an approved DoD encryption package and enable full disk encryption on mobile systems.		
		V-63801	WN10-SO-000205	BitLocker can be enabled in "BitLocker Drive Encryption" in the Control Panel.	140	findows
		V-63847	WN10-UR-000015			Linux
		V-63859	WN10-UR-000045	References		
		V-63869	WN10-UR-000065	CCE: CCI-001199: The information system protects the confidentiality and/or integrity of organization-defined information at rest.	Last Updatest	I hour ago
		NISTS P800-33 = 50-20 NISTS P800-33 = 52-20		NIST SP 800-53 = SC-28 NIST SP 800-53A = SC-28.1	SCAP Audit	Summary - I
				NIST SP 800-53 Revision 4 :: SC-28		
				CCI-002475: The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-	IP Address	s Score
				defined information at rest on organization-defined information system components. NIST SP 800-53 Revision 4 : SC 28 (1)	10.31.104.0	/24
					172.26.48.0	0/24
	Remove Filter(s) Remove All Filters	Showing rule 1 out of 27		CCI 002476: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization- defined information at rest on organization-defined information system components.		

SCAP A	udit Sum	mary						BB Switch
SCAP Audit S	ummary - Top 25	Linux Compliance Failed Cl	hecks		>	SCAP Audt S	lummary - Top 25 Windows Compliance Failed Checks	
Plugin ID	Name Se	verity Total				Plugin ID	Name	Severit
1003887	CCE-18031-5-3	psec_tools_package/USGC	8-RHEL-S-Desktop_12.5.0 ur	ited_states_povernment_configurati_	Hot 1	10046	CCE-M830-4:SV-25139rt_nuie:Windows_7_STIG_tMAC-1_Public	High
10038	CCE-17504-2:	irda_tools_package:USGCB	HHEL-5-Desktop_12.5.0:uni	ted_states_povernment_configurati	High 1	10046	CCE-14109-3:SV-25138rt_rule:Windows_7_STIG_1MAC-L_Public	High
10038_	CCE-18200-6:	talk_package:USGCB-RHEL	-5-Desktop_12.5.0 united_st	ates_government_configuration_ba	High 1	10046	noCCE The Enhanced Mitigation Experience Toolkit (EMET) must be installed on the system VMS 1	Target W., High
10038	CCE-17250-2:	pam_ccreds_package/USG	CB-RHEL-5-Desktop_12.5.0:	inited_states_povernment_configura_	High 1	10046	CCE-IS041-7:SV-25143rt_ruleWindows_7_STIG_1MAC-1_Public	High
10038	CCE-17742-8:1	usgcb-mel5desktop-rule-2.6	1.0.USGC8-RHEL-S-Desktop	12.5.0 united_states_government	High 1	10046	CCE-10777-1:SV-25107r1_rule:Windows_7_STIG_13MAC-1_Public	High
1003881	3881 CCE-15018-5:postfix_network_listening:USGCB-RHEL-5-Desktop_12.5.0:united_states_government_config_			Hgh 1	10046	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) system wide Address Space Layout Ri	landomizat High	
10038 CCE-14068-1:postfix_package_installation:USOCB-RHEL-S-Desklop_12.5.0 united_states_government_co						10046	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention	on (DEP) High
10038	CCE-54495-6:	sendmail_package_installet	ion:USGC8-RHEL-5-Desktop	12.5.0 united_states_government	High 1	1004641	noCCE: The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Softwa	are is not e High
1003878	CCE-14825-4:	isdn4k_utils_package/USGC	28-RHEL-S-Desktop_12.5.0.	nited_states_government_configura.	Hgh 1	10046	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explore	rer must b High
10038	CCE-14412-1:m	odev_option_on_tmp:USGC	CB-RHEL-5-Desktop_12.5.0%	nited_states_government_configura.	High 1	10046	noCCELocal administrator accounts must have their privileged token filtered to prevent elevated p	privlegesHigh
Lest Updated: 1	hour ago					Lest Updeted: 1	hour ago	
SCAP Audit S	ummary - Compile	ance Summary				SCAP Audit S	summary - Top 10 CCE's	
		Systems	Passed	Manual Check	Failed	2	Metur Hap	Plant Total
	idows inux	1	30%	25	674	1.8		
Last Updated: 1			22%	ian i		14		
SCAP Audit S	ummary - Networ	k Summary			>	1		
		nfo Medium High	Total			0.6		

SCAP Compliance Checker

The SCAP Compliance Checker is an automated compliance scanning tool that leverages the DISA Security Technical Implementation Guidelines (STIGs) and operating system (OS) specific baselines to analyze and report on the security configuration of an information system. The tool can be run locally on the host system to be scanned, or scans can be conducted across a network from any machine on the domain. In either scanning environment, the following requirement applies: The user conducting the scan must have administrative privileges on the machine to be scanned. If the machine to be scanned is not hosting the tool, domain-level administrative privileges (or individual local administrator accounts) are required to remotely scan other systems on the network.

+

Agenda

- ✓ Risk Management Framework A quick review...
- ✓ Implementing controls Host hardening...
 - ✓ Security configuration checklist (with STIG Viewer)

✓ SCAP - Security Content Automation Protocol

- System Security Plan's Appendix 1
 - Select 1 Technical control family to fill out for your information system
- System Security Plan's System Information
 - Information System Type
- Team Project SSP draft development...

SSP – Table of Contents

TABLE OF CONTENTS

	1	Introduction	8
	2	Purpose	8
	3	System Information	
	4	System Owner	10
	5	Assignment of Security Responsibility	11
	6	Leveraged FedRAMP-Authorized Services	
	7	External Systems and Services Not Having FedRAMP Authorization	15
1	8	Illustrated Architecture and Narratives	19
		8.1 Illustrated Architecture	19
		8.2 Narrative	22
	9	Services, Ports, and Protocols	24
	10	Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)	27
	11	Separation of Duties	29
	12	SSP Appendices List	31
	Ар	pendix A <insert cso="" name=""> FedRAMP Security Controls</insert>	33
	Ap	pendix B <insert cso="" name=""> Related Acronyms</insert>	35
	Ap	pendix C <insert cso="" name=""> Information Security Policies and Procedures</insert>	36
	Ap	pendix D <insert cso="" name=""> User Guide</insert>	37
	Ap	pendix E <insert cso="" name=""> Digital Identity Worksheet</insert>	37
	Ap	pendix F <insert cso="" name=""> Rules of Behavior (RoB)</insert>	40
	Ap	pendix G <insert cso="" name=""> Information System Contingency Plan (ISCP)</insert>	40
	Ap	pendix H <insert cso="" name=""> Configuration Management Plan (CMP)</insert>	41
	Ap	pendix I <insert cso="" name=""> Incident Response Plan (IRP)</insert>	42
	Аp	pendix J <insert cso="" name=""> Control Implementation Summary (CIS) and Customer Responsibilities Matrix (CRM) Workbook</insert>	43
	Ap	pendix K <insert cso="" name=""> Federal Information Processing Standard (FIPS) 199 Categorization</insert>	44
	Ap	pendix L <insert cso="" name="">-Specific Laws and Regulations</insert>	47
	Ap	pendix M <insert cso="" name=""> Integrated Inventory Workbook (IIW)</insert>	47

Appendix N <insert cso="" name=""> Continuous Monitoring Plan</insert>	. 48
Appendix O <insert cso="" name=""> POA&M</insert>	.49
Appendix P <insert cso="" name=""> Supply Chain Risk Management Plan (SCRMP)</insert>	.49
Appendix Q <insert cso="" name=""> Cryptographic Modules Table</insert>	.50

SSP's Technical Controls: SSP's Appendix A

NIST Special Publication 800-18 Revision 1

NIST

National Institute of Standards and Technology Technology Administration U.S. Department of Commerce Marianne Swanson Joan Hash Pauline Bowen

Guide for Developing Security Plans for Federal Information

INFORMATION SECURITY

Systems

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

February 2006



U.S. Department of Commerce Carlos M.Gutierres, Secretary

National Institute of Standards and Technology William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER		
Management	Risk Assessment	RA		
Management	Planning	PL		
Management	System and Services Acquisition	SA		
Management	Certification, Accreditation, and Security Assessments	CA		
Operational	Personnel Security	PS		
Operational	Physical and Environmental Protection	PE		
Operational	Contingency Planning	CP		
Operational				
Operational	Maintenance	MA		
Operational	System and Information Integrity	SI		
Operational	Media Protection	MP		
Operational	Incident Response	IR		
Operational	Awareness and Training	AT		
Technical	Identification and Authentication	IA		
Technical	Access Control	AC		
Technical	Audit and Accountability	AU		
Technical	System and Communications Protection	SC		

Table 2: Security Control Class, Family, and Identifier

Technical Controls

NIST Special Publication 800-18 Revision 1

Guide for Developing Security Plans for Federal Information Systems



National Institute of Standards and Technology Technology Administration U.S. Department of Commerce Marianne Swanson Joan Hash Pauline Bowen

INFORMATION SECURITY

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

February 2006



U.S. Department of Commerce Carlos M.Gutierres, Secretary

National Institute of Standards and Technology William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. **FIPS PUB 200**

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

March 2006



U.S. DEPARTMENT OF COMMERCE Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY William Jeffrey, Director



FedRAMP[®] System Security Plan (SSP) Appendix A: High FedRAMP Security Controls

for <Insert CSP Name>

<Insert CSO Name>

<Insert Version X.X>

<Insert MM/DD/YYYY>



Controlled Unclassified Information

info@fedramp.gov fedramp.gov



FedRAMP[®] System Security Plan (SSP) Appendix A: High FedRAMP Security Controls <insert CSP Name> | <insert CSO Name> | <insert Version X.X | <insert MM/DD/YYY>

CP-9(2) Test Restoration Using Sampling (H)	228
CP-9(3) Separate Storage for Critical Information (H)	
CP-9(5) Transfer to Alternate Storage Site (H)	231
CP-9(8) Cryptographic Protection (M)(H)	
CP-10 System Recovery and Reconstitution (L)(M)(H)	233
CP-10(2) Transaction Recovery (M)(H)	234
CP-10(4) Restore Within Time Period (H)	
Identification and Authentication	
IA-1 Policy and Procedures (L)(M)(H)	236
IA-2 Identification and Authentication (Organizational Users) (L)(M)(H)	238
IA-2(1) Multi-factor Authentication to Privileged Accounts (L)(M)(H)	
IA-2(2) Multi-factor Authentication to Non-privileged Accounts (L)(M)(H)	240
IA-2(5) Individual Authentication with Group Authentication (M)(H)	
IA-2(6) Access to Accounts —separate Device (M)(H)	243
IA-2(8) Access to Accounts — Replay Resistant (L)(M)(H)	244
IA-2(12) Acceptance of PIV Credentials (L)(M)(H)	
IA-3 Device Identification and Authentication (M)(H)	246
IA-4 Identifier Management (L)(M)(H)	247
IA-4(4) Identify User Status (M)(H)	
IA-5 Authenticator Management (L)(M)(H)	
IA-5(1) Password-based Authentication (L)(M)(H)	
IA-5(2) Public Key-based Authentication (M)(H)	
IA-5(6) Protection of Authenticators (M)(H)	
IA-5(7) No Embedded Unencrypted Static Authenticators (M)(H)	257

FR.

FedRAMP[®] System Security Plan (SSP) Appendix A: High FedRAMP Security Controls <Insert CSP Name> | <Insert CSD Name> | <insert Version X.X. | <Insert MMDD/YYY>

IA-5(8) Multiple System Accounts (H)	8
IA-5(13) Expiration of Cached Authenticators (H)	9
IA-8 Authentication Feedback (L)(M)(H)	0
IA-7 Cryptographic Module Authentication (L)(M)(H)26	i1
IA-8 Identification and Authentication (Non-organizational Users) (L)(M)(H)26	2
IA-8(1) Acceptance of PIV Credentials from Other Agencies (L)(M)(H)26	3
IA-8(2) Acceptance of External Authenticators (L)(M)(H)	64
IA-8(4) Use of Defined Profiles (L)(M)(H)	5
IA-11 Re-authentication (L)(M)(H)	6
IA-12 Identity Proofing (M)(H)	8
IA-12(2) Identity Evidence (M)(H)	9
IA-12(3) Identity Evidence Validation and Verification (M)(H)27	0
IA-12(4) In-person Validation and Verification (H)27	'1
IA-12(4) In-person Validation and Verification (H)	
	'2
IA-12(5) Address Confirmation (M)(H)27	'2 '3
IA-12(5) Address Confirmation (M)(H)	'2 '3 '3
IA-12(5) Address Confirmation (M)(H)	'2 '3 '3
IA-12(5) Address Confirmation (M)(H)	'2 '3 '5 '6
IA-12(5) Address Confirmation (M)(H) .27 Incident Response .27 IR-1 Policy and Procedures (L)(M)(H) .27 IR-2 Incident Response Training (L)(M)(H) .27 IR-2(1) Simulated Events (H) .27	'2 '3 '5 '6
IA-12(5) Address Confirmation (M)(H)	'2 '3 '5 '7 '9
IA-12(5) Address Confirmation (M)(H) .27 Incident Response .27 IR-1 Policy and Procedures (L)(M)(H) .27 IR-2 Incident Response Training (L)(M)(H) .27 IR-2(1) Simulated Events (H) .27 IR-2(2) Automated Training Environments (H) .27 IR-3 Incident Response Testing (M)(H) .27	72 73 75 76 77 79
IA-12(5) Address Confirmation (M)(H) .27 Incident Response .27 IR-1 Policy and Procedures (L)(M)(H) .27 IR-2 Incident Response Training (L)(M)(H) .27 IR-2 Incident Response Training (L)(M)(H) .27 IR-2(1) Simulated Events (H) .27 IR-2(2) Automated Training Environments (H) .27 IR-3 Incident Response Testing (M)(H) .27 IR-3(2) Coordination with Related Plans (M)(H) .28	72 73 75 76 77 79

Identification and Authentication (IA)

CNTL		PRIORITY	INITIAL CONTROL BASELINES			
NO.	CONTROL NAME		LOW	MOD	нідн	
	Identification	and Au	thentication			
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1	
IA-2	Identification and Authentication (Organizational Users)		IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)	
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3	
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4	
IA-5	Authenticator Management		IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)	
IA-6	Authenticator Feedback		IA-6	IA-6	IA-6	
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7	
IA-8	Identification and Authentication (Non- Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	

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

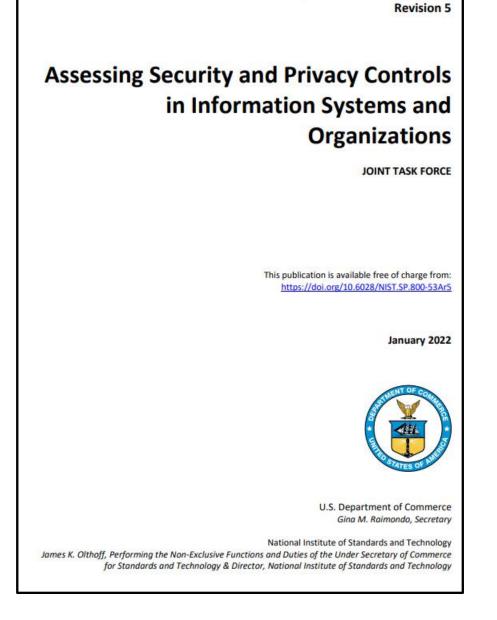
IA-1 Identification and Authentication Policy and Procedures

<u>Control</u>: The organization:

- a. Develops, documents, and disseminates to [Assignment: organizationdefined personnel or roles]:
 - 1. An identification and authentication policy that addresses **purpose**, **scope**, **roles**, **responsibilities**, **management commitment**, **coordination among organizational entities**, **and compliance**; and
 - 2. Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls; and
- b. Reviews and updates the current:
 - a. Identification and authentication policy [Assignment: organization-defined frequency]; and
 - b. Identification and authentication procedures [Assignment: organization-defined frequency].

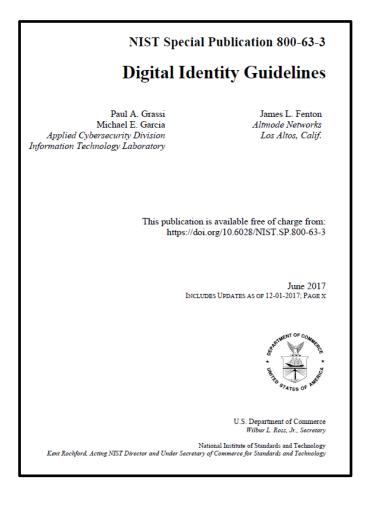
IDENTIFICA	TION AND AUTH	ENTICATION POLIC	CY AND PROCEDURES			
ASSESSME	NT OBJECTIVE:					
Determine	if the organiza	ition:				
IA-1(a)(1)	IA-1(a)(1)[1]	develops and d policy that add	ocuments an identification and authentication resses:			
		IA-1(a)(1)[1][a]	purpose;			
		IA-1(a)(1)[1][b]	scope;			
		IA-1(a)(1)[1][c]	roles;			
		IA-1(a)(1)[1][d]	responsibilities;			
		IA-1(a)(1)[1][e]	management commitment;			
		IA-1(a)(1)[1][f]	coordination among organizational entities;			
		IA-1(a)(1)[1][g]	compliance;			
	IA-1(a)(1)[2]		nel or roles to whom the identification and policy is to be disseminated; and			
	IA-1(a)(1)[3]	disseminates the identification and authentication policy to organization-defined personnel or roles;				
IA-1(a)(2)	IA-1(a)(2)[1]	develops and documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls;				
	IA-1(a)(2)[2]	defines personnel or roles to whom the procedures are to be disseminated;				
	IA-1(a)(2)[3]	disseminates the procedures to organization-defined personnel or roles;				
IA-1(b)(1)	IA-1(b)(1)[1]		nuency to review and update the current nd authentication policy;			
	IA-1(b)(1)[2]	reviews and updates the current identification and authenticati policy with the organization-defined frequency; and				
IA-1(b)(2)	IA-1(b)(2)[1]	defines the frequency to review and update the current identification and authentication procedures; and				
	IA-1(b)(2)[2]		dates the current identification and authentication h the organization-defined frequency.			
POTENTIAL	ASSESSMENT	METHODS AND OB.	JECTS:			
	SELECT FROM: Ide		entication policy and procedures; other relevant			
			anel with identification and authentication responsibilities; ation security responsibilities].			

IA-1



NIST Special Publication 800-53A

IA-1 Identification and Authentication Policy and Procedures



University of Wisconsin Superior	Identification and Authentication Policy and Procedures		
Department Name Technology Services	Policy # IT-IA1	Issue Date: March 16, 2016	
Approved by:			

1. Purpose

The University of Wisconsin Superior fosters intellectual growth and career preparation within a liberal arts tradition that emphasizes individual attention, embodies respect for diverse cultures and multiple voices, and engages the community and region. This policy establishes the Identification and Authentication Policy and Procedures. This policy addresses the establishment of procedures for the effective implementation of selected security controls and control enhancements in the Identification and Authentication Policy and Procedures Family.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by the University of Wisconsin Superior. Any information, not specifically identified as the property of other parties, that is transmitted or stored on University of Wisconsin Superior IT resources (including e-mail, messages and files) is the property of the University of Wisconsin Superior. All users (University of Wisconsin Superior employees, Students, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Data Classification

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). Access Controls will vary depending upon the following classifications:

Level I: Low Sensitivity/Public Data:

Access to Level I institutional data is targeted for general public use and may be granted to any requester or may be published with no restrictions. Level I data is specifically defined as public in local, state, or federal law, or data whose original purpose was for public disclosure.

Examples of Level I (low sensitivity) institutional data:

- · published "white pages" directory information
- maps
- · university websites intended for public use
- · course catalogs and schedules of classes (timetables)
- · campus newspapers, magazines, or newsletters
- press releases
- campus brochures

Level III: Moderate Sensitivity/Internal Data:

Access to Level III institutional data is authorized for all employees for business purposes unless restricted by a data steward. Access to data of this level is generally not available to parties outside the university community and must be requested from, and authorized by, the data steward who is responsible for the data.

Identification and Authentication (IA)

CNTL		PRIORITY	INITIAL CONTROL BASELINES			
NO.	CONTROL NAME		LOW	MOD	HIGH	
	Identification	and Au	thentication			
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1	
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)	
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3	
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4	
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)	
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6	
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7	
IA-8	Identification and Authentication (Non- Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	

NIST Special Publication 800-53 Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

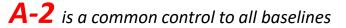
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

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



IA-2 Identification and Authentication (Organizational Users)

<u>Control</u>: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational

users)

IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
	ASSESSMENT OBJECTIVE:
	Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records].
	Interview: [SELECT FROM: Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers].
	Test: [SELECT FROM: Organizational processes for uniquely identifying and authenticating users; automated mechanisms supporting and/or implementing identification and authentication capability].

TABLE OF CONTENTS

1 Introduction.. 2 Purpose.....

2	Purpose	ŏ
3	System Information	8
4	System Owner	10
5	Assignment of Security Responsibility	11
6	Leveraged FedRAMP-Authorized Services	12
7	External Systems and Services Not Having FedRAMP Authorization	15
8	Illustrated Architecture and Narratives	19
	8.1 Illustrated Architecture	19
	8.2 Narrative	22
9	Services, Ports, and Protocols	24
10	Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)	27
11	Separation of Duties	



4

5

- 6

...8

FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP <Insert CSP Name> | <Insert CSO Name> | <Insert Version XX> | <Insert MM/DD/YYY>

Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

System Information	
CSP Name:	<insert csp="" name=""> <insert abbreviation,="" appropriate="" as="" csp=""></insert></insert>
CSO Name:	<insert cso="" name=""> <insert abbreviation,="" appropriate="" as="" cso=""></insert></insert>
FedRAMP Package ID:	<insert fedramp="" id="" package=""></insert>
Service Model:	<choose iaas="" iaas,="" one:="" paas="" paas,="" saas,="" saas,<br="">IaaS/SaaS, PaaS/SaaS, LI-SaaS></choose>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<choose aal1="" aal2,="" aal3,="" fal1="" fal2="" fal3="" ial1="" ial2="" ial3="" one:=""></choose>
FIPS PUB 199 Level (SSP Appendix K):	<choose high,="" li-saas="" low,="" moderate,="" one:=""></choose>
Fully Operational as of:	<insert dd="" mm="" yyyy=""></insert>
Deployment Model:	<choose cloud="" cloud,="" government-only="" hybrid="" one:="" public=""></choose>
Authorization Path:	<choose agency="" authorization="" authorization,="" board="" joint="" one:="" provisional=""></choose>
General System Description:	<insert cso="" name=""> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and</insert>

		Assurance Level	
Impact Categories	1	2	3
Inconvenience, distress or damage to standing or reputation	Low	Mod	High
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

Business Area	Business Area ID		Inconvenience, distress or damage to standing or reputation	Financial loss or	nrograms	Unauthorized release of sensitive information	Personal Safety	Civil or criminal violations	IAL	AAI
Environmental Management	D.8	Pollution Prevention and Control	Low	Low	Low	Low	Low	Low		
Public Goods Creation & Management	D.22	Public Resources, Facility and Infrastructure Management	Moderate	Low	Low	Moderate	Low	Low		
		Tenant Data	Moderate	Low	Low	Moderate	Low	Low		
Information & Technology Management	C.3.5.5	Information Security	Moderate	Low	Moderate	Moderate	Low	Low		
Information & Technology Management	C.3.5.6	Record Retention	Moderate	Low	Moderate	Moderate	Low	Low	_	
Information & Technology Management	C.3.5.7	Information Management	Moderate	Low	Moderate	Moderate	Low	Low	2	2
Information & Technology Management	C.3.5	System and Network Monitoring	Moderate	Low	Moderate	Moderate	Low	Low		
		System Data	Moderate	Low	Moderate	Moderate	Low	Low		
			Moderate	Low	Moderate	Moderate	Low	Low		
		Assurance Level:	2	1	2	2	2	2		

SSP – Table of Contents

TABLE OF CONTENTS

	1	Introduction	8
	2	Purpose	8
Γ	3	System Information	8
_	4	System Owner	10
	5	Assignment of Security Responsibility	11
	6	Leveraged FedRAMP-Authorized Services	12
	7	External Systems and Services Not Having FedRAMP Authorization	15
	8	Illustrated Architecture and Narratives	19
		8.1 Illustrated Architecture	19
		8.2 Narrative	22
	9	Services, Ports, and Protocols	24
	10	Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)	27
	11	Separation of Duties	29
	12	SSP Appendices List	31
	Ap	pendix A <insert cso="" name=""> FedRAMP Security Controls</insert>	33
	Ap	pendix B <insert cso="" name=""> Related Acronyms</insert>	35
	Ap	pendix C <insert cso="" name=""> Information Security Policies and Procedures</insert>	36
	Ap	pendix D <insert cso="" name=""> User Guide</insert>	37
	Ap	pendix E <insert cso="" name=""> Digital Identity Worksheet</insert>	37
	Ap	pendix F <insert cso="" name=""> Rules of Behavior (RoB)</insert>	40
	Ap	pendix G <insert cso="" name=""> Information System Contingency Plan (ISCP)</insert>	40
	Ap	pendix H <insert cso="" name=""> Configuration Management Plan (CMP)</insert>	41
	Ap	pendix I <insert cso="" name=""> Incident Response Plan (IRP)</insert>	42
	Ap	pendix J <insert cso="" name=""> Control Implementation Summary (CIS) and Customer Responsibilities Matrix (CRM) Workbook</insert>	43
	Ap	pendix K <insert cso="" name=""> Federal Information Processing Standard (FIPS) 199 Categorization</insert>	44
	Ap	pendix L <insert cso="" name="">-Specific Laws and Regulations</insert>	47
	Ap	pendix M <insert cso="" name=""> Integrated Inventory Workbook (IIW)</insert>	47

Appendix N <insert cso="" name=""> Continuous Monitoring Plan</insert>	48
Appendix O <insert cso="" name=""> POA&M</insert>	49
Appendix P <insert cso="" name=""> Supply Chain Risk Management Plan (SCRMP)</insert>	49
Appendix Q <insert cso="" name=""> Cryptographic Modules Table</insert>	50

Appendix E <Insert CSO Name> Digital Identity Worksheet

Instruction:

This appendix applies to all baselines (LI-SaaS, Low, Moderate, and High).

Complete Table E.2, below; a separate attachment is not required. Authentication solutions, provided by a CSP for CSP-personnel to access and administer the CSO, must meet digital identity requirements. Authentication solutions provided by a CSP, for customers to access the CSO, must also meet digital identity requirements.

Delete this note and all other instructional text from your final version of this document.

Mapping FedRAMP Levels to NIST SP 800-63 Levels

Digital identity is the process of establishing confidence in user identities electronically presented to an information system. Authentication focuses on the identity proofing process, the authenticator management process, and the assertion protocol used in a federated environment to communicate authentication and attribute information, if applicable.

Table E.1, below, "Mapping FedRAMP Levels to NIST SP 800-63 Levels", maps the FedRAMP impact levels (Low/LI-SaaS, Moderate, and High) to <u>NIST SP 800-63 Digital Identity Guidelines</u> levels]

- · Identity Assurance Level (IAL) Refers to the identity proofing process
- Authenticator Assurance Level (AAL) Refers to the authentication process
- Federation Assurance Level (FAL) Refers to the strength of an assertion in a federated environment, used to communicate authentication and attribute information (if applicable), to a relying party (RP)

Table E.1 Mapping FedRAMP Levels to NIST SP 800-63 Levels

R

FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP)

FedRAMP Impact Level	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
High	IAL3: In-person or supervised remote identity proofing	AAL3: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography; authenticator must be hardware-based	FAL3: The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it. For very high value or very high risk situations, the subscriber (user) must provide proof of possession of a secure, cryptographic key, and a HW based device to provide verifier impersonation resistance. The device may fulfill both requirements.
Moderate	IAL2: In-person or remote, potentially involving a "trusted referee"	AAL2: Multi-factor required; authenticators and verifiers use FIPS 140-validated cryptography	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Low and FedRAMP LI-SaaS	IAL1: Self-asserted	AAL1: Single-factor or multi-factor; verifiers use FIPS 140-validated cryptography	FAL1: Assertion is digitally signed by the identity provider

Digital Identity Level Selection

FR

FedRAMP® (High, Moderste, Low, LI-SaaS) Baseline System Security Plan (SSP) <Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

Instructions:

Select the lowest level that will cover all potential impacts identified from the table above.

Delete this and all other instructional text from your final version of this document.

The <Insert CSP Name> has identified that they support the digital identity level that has been selected for the <Insert CSO Name>. The selected digital identity level indicated is supported for federal agency consumers of the CSO. Implementation details of the digital identity mechanisms are provided in Appendix A under control IA-2.

Table E.2 Digital Identity Level

Digital Identity Level	Maximum Impact Profile	Selection
Level 1: AAL1, IAL1, FAL1	Low/LI-SaaS	
Level 2: AAL2, IAL2, FAL2	Moderate	
Level 3: AAL3, IAL3, FAL3	High	

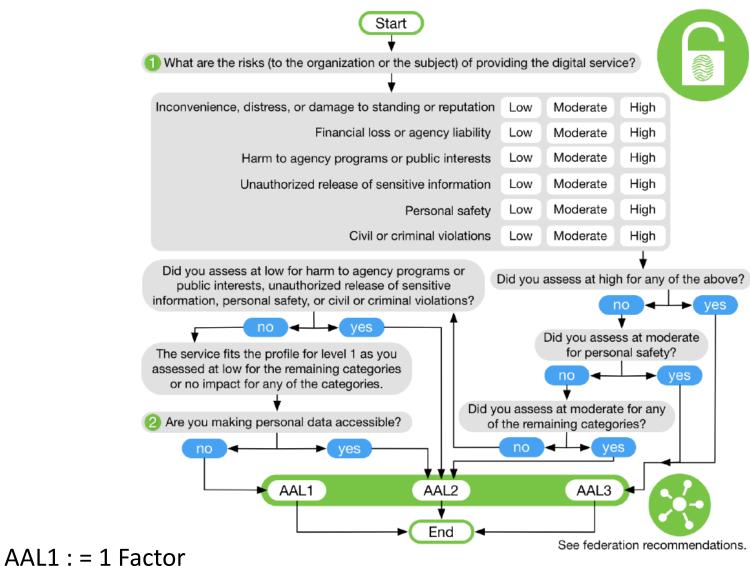
IA-2 Identification and Authentication

Control Enhancement:

IA-2(1)	IDENTIFICATION AND AUTHENTICATION NETWORK ACCESS TO PRIVILEGED ACCOUNTS
	ASSESSMENT OBJECTIVE:
	Determine if the information system implements multifactor authentication for network access to privileged accounts.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records].
	Interview: [SELECT FROM: Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers].
	Test: [SELECT FROM: Automated mechanisms supporting and/or implementing multifactor authentication capability].

Requirement	AAL1	AAL2	AAL3	
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret	
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)	
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors	
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)	
MitM Resistance	Required	Required	Required	
Verifier- Impersonation Resistance	Not required	Not required	Required Required	
Verifier- Compromise Resistance	Not required	Not required		
Replay Resistance	Not required	Not required	Required	
Authentication Intent	Not required	Recommended	Required	
Records Retention Policy	Required	Required	Required	
Privacy Controls	Required	Required	Required	

Authenticator Assurance



AAL = Authenticator Assurance Level

AAL3 : = 2 Factors: Hardware-based authenticator and an authenticator that provides verifier impersonation resistance

AAL2 := 2 Factors

Agenda

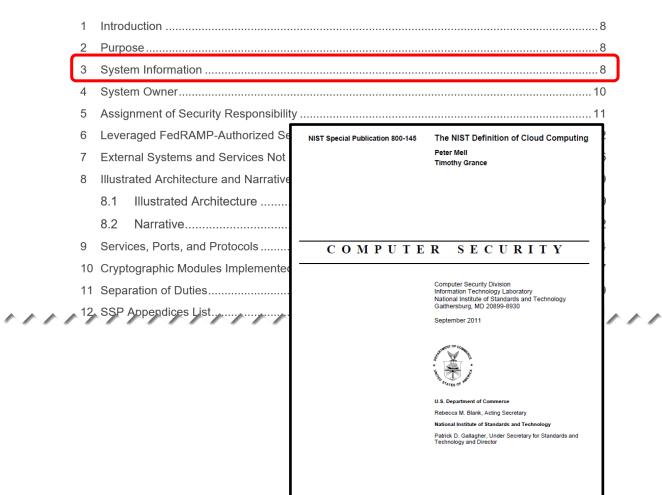
- ✓ Risk Management Framework A quick review...
- ✓ Implementing controls Host hardening...
 - ✓ Security configuration checklist (with STIG Viewer)
- ✓ SCAP Security Content Automation Protocol
- ✓ System Security Plan's Appendix 1
 - ✓ Select 1 Technical control family to fill out for your information system
- System Security Plan's System Information
 - Information System Type
- Team Project SSP draft development...

SSP – Table of Contents



FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP) <Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

TABLE OF CONTENTS



FR.

FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP) dnsert CSP Name> | <insert CSO Name> | <insert Version X.X> | <insert MM/DD/YYY>

Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

CSP Name:	<insert csp="" name=""> <insert abbreviation,="" appropriate="" as="" csp=""></insert></insert>	
CSO Name:	<insert cso="" name=""> <insert abbreviation,="" appropriate="" as="" cso=""></insert></insert>	
FedRAMP Package ID:	<insert fedramp="" id="" package=""></insert>	
Service Model:	<choose laas="" laas,="" one:="" paas="" paas,="" saas,="" saas,<br="">laaS/SaaS, PaaS/SaaS, LI-SaaS></choose>	
Digital Identity Level (DIL) Determination (SSP Appendix E):	<choose aal1="" aal2,="" aal3,="" fal1="" fal2="" fal3="" ial1="" ial2="" ial3="" one:=""></choose>	
FIPS PUB 199 Level (SSP Appendix K):	<choose high,="" li-saas="" low,="" moderate,="" one:=""></choose>	
Fully Operational as of:	<insert dd="" mm="" yyyy=""></insert>	
Deployment Model:	<choose cloud="" cloud,="" government-only="" hybrid="" one:="" public=""></choose>	
Authorization Path:	<choose authorization="" authorization,<br="" board="" joint="" one:="" provisional="">Agency Authorization></choose>	
General System Description:	<insert cso="" name=""> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].</insert>	



TABLE OF CONTENTS

	1	Introduction
2	2	Purpose
	3	System Information
4	4	System Owner10
ļ	5	Assignment of Security Responsibility
6	6	Leveraged FedRAMP-Authorized Services
7	7	External Systems and Services Not Having FedRAMP Authorization
8	3	Illustrated Architecture and Narratives
		8.1 Illustrated Architecture
		8.2 Narrative
ę	9	Services, Ports, and Protocols
	10	Cryptographic Modules Implemented for Data At Rest (DAR) and Data In Transit (DIT)27
	11	Separation of Duties

Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

		System Information	
		CSP Name:	<insert csp="" name=""> <insert abbreviation,="" appropriate="" as="" csp=""></insert></insert>
		CSO Name:	<insert cso="" name=""> <insert abbreviation,="" appropriate="" as="" cso=""></insert></insert>
		FedRAMP Package ID:	<insert fedramp="" id="" package=""></insert>
		Service Model:	<choose iaas="" iaas,="" li-saas="" one:="" paas="" paas,="" saas,=""></choose>
		Digital Identity Level (DIL) Determination (SSP Appendix E):	<choose aal1="" aal2,="" aal3,="" fal1="" fal2="" fal3="" ial1="" ial2="" ial3="" one:=""></choose>
			<choose high,="" li-saas="" low,="" moderate,="" one:=""></choose>
ST Special Publication 800-145 The NIST Definition of Cloud Computing Peter Mell		Fully Operational as of:	<insert dd="" mm="" yyyy=""></insert>
Timothy Grance		Deployment Model:	<choose cloud="" cloud,="" government-only="" hybrid="" one:="" public=""></choose>
		Authorization Path:	<choose authorization="" authorization,<br="" board="" joint="" one:="" provisional="">Agency Authorization></choose>
COMPUTER SEC	URITY	General System	<insert cso="" name=""> is delivered as [a/an] [insert based on the</insert>
Computer Security Di Information Technolog	vision jy Laboratory tandards and Technology	Description:	Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].

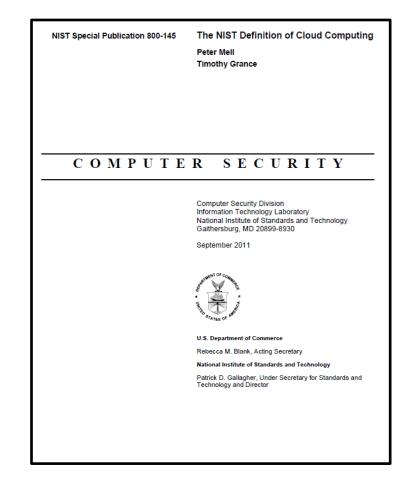


NIST Special Publication 800-145

U.S. Department of Commerce Rebecca M. Blank, Acting Secretary National Institute of Standards and Technology Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Essential Characteristics of Cloud Computing

- 1. On-demand self-service
- 2. Broad network access
- 3. Resource pooling
- 4. Rapid elasticity
- 5. Measured service



Cloud Service Models

Infrastructure as a Service (IaaS)

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications
- The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)

Platform as a Service (PaaS)

- The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment

Software as a Service (SaaS)

- The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings

Cloud Deployment Models

Private cloud

- The cloud infrastructure is provisioned for <u>exclusive use by a single organization</u> comprising multiple consumers (e.g., business units)
- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

Community cloud

- The cloud infrastructure is provisioned for <u>exclusive use by a specific community of consumers from</u> organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)
- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises

Public cloud

- The cloud infrastructure is provisioned for open use by the general public
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider

Hybrid cloud

The cloud infrastructure is a <u>composition of two or more distinct cloud infrastructures</u> (private, community, or public) <u>that remain unique entities</u>, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

Service Provider Cloud Deployment Model				
	Public	Cloud services and infrastructure supporting multiple organizations and agency clients		
	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients		
	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations		
	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.		



Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

CSP Name:	<insert csp="" name=""> <insert abbreviation,="" appropriate="" as="" csp=""></insert></insert>	
CSO Name:	<insert cso="" name=""> <insert abbreviation,="" appropriate="" as="" cso=""></insert></insert>	
FedRAMP Package ID:	<insert fedramp="" id="" package=""></insert>	
Service Model:	<choose laas="" laas,="" one:="" paas="" paas,="" saas,="" saas,<br="">laaS/SaaS, PaaS/SaaS, LI-SaaS></choose>	
Digital Identity Level (DIL) Determination (SSP Appendix E):	<choose aal1="" aal2,="" aal3,="" fal1="" fal2="" fal3="" ial1="" ial2="" ial3="" one:=""></choose>	
FIPS PUB 199 Level (SSP Appendix K):	<choose high,="" li-saas="" low,="" moderate,="" one:=""></choose>	
Fully Operational as of:	<insert dd="" mm="" yyyy=""></insert>	
Deployment Model:	<choose cloud="" cloud,="" government-only="" hybrid="" one:="" public=""></choose>	
Authorization Path:	<choose authorization="" authorization,<br="" board="" joint="" one:="" provisional="">Agency Authorization></choose>	
General System Description:	<insert cso="" name=""> is delivered as [a/an] [insert based on the Service Model above] offering using a multi-tenant [insert based on the Deployment Model above] cloud computing environment. It is available to [Insert scope of customers in accordance with instructions above (for example, the public, federal, state, local, and tribal governments, as well as research institutions, federal contractors, government contractors etc.)].</insert>	

Agenda

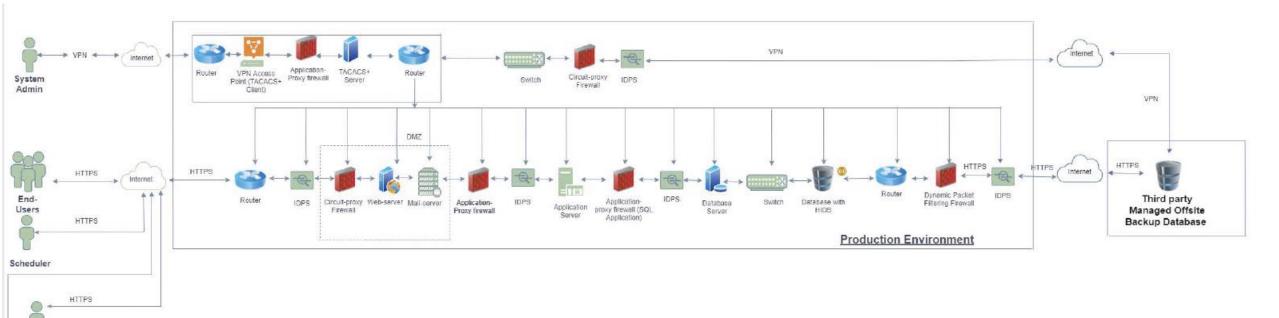
- ✓ NIST Risk Management Framework A quick review...
- ✓ Implementing controls Host hardening...
 - ✓ Security configuration checklist (w/DISA STIG Viewer)
- ✓ NIST 800-53Ar4 How Controls are Assessed
- ✓ SCAP Security Content Automation Protocol
- ✓ FedRAMP System Security Plan's Section 13 A controls deep dive
 ✓ Identity and Authentication controls assessment questions
- ✓ System Security Plan's Section 8
 - ✓ Information System Type
- Team Project SSP drafts...

Next Class – Logical diagrams

Unit #	Team Project Schedule	
8	1 st Rough Draft System Security Plan (SSP) review	3/13
10	2 nd Draft SSP review	3/27
11	3 rd Draft SSP review	4/3

- Network diagram depicting locations and relationships among:
 - Servers
 - Security components
 - Internet
 - Users
 - Interconnected systems
- Boundary diagram network diagram that also depicting boundaries and flow of data across interconnections that cross internal and external boundaries:
 - Security zones
 - Internal Interconnections to external systems
- Data flow (simplified) a series of individual boundary diagrams that also depict data flowing to/from individual classes of users that enable seeing how their data packets are secured as they flow across the boundaries and through the logical network
 - End users
 - System administrators
 - Testers
 - Developers

What can be improved in this security architecture?



U

Tester

Agenda

- ✓ Risk Management Framework A quick review...
- ✓ Implementing controls Host hardening...
 - ✓ Security configuration checklist (with STIG Viewer)
- ✓ SCAP Security Content Automation Protocol
- ✓ System Security Plan's Section 13
 - ✓ Select 1 control family to fill out for your information system
- ✓ System Security Plan's Section 8
 - ✓Information System Type
- ✓ Team Project SSP draft development...