Unit #9

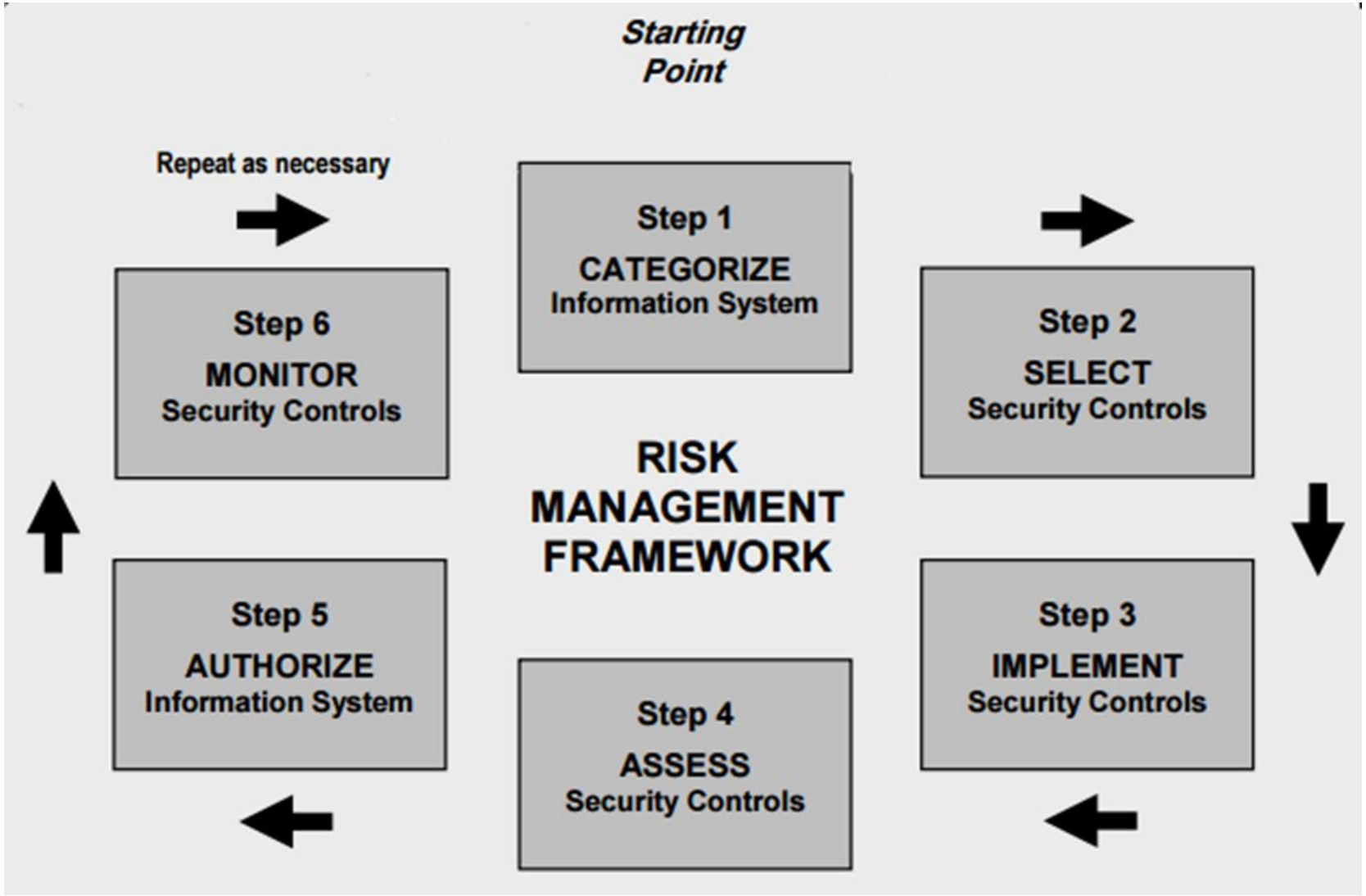
MIS5214

Host Hardening

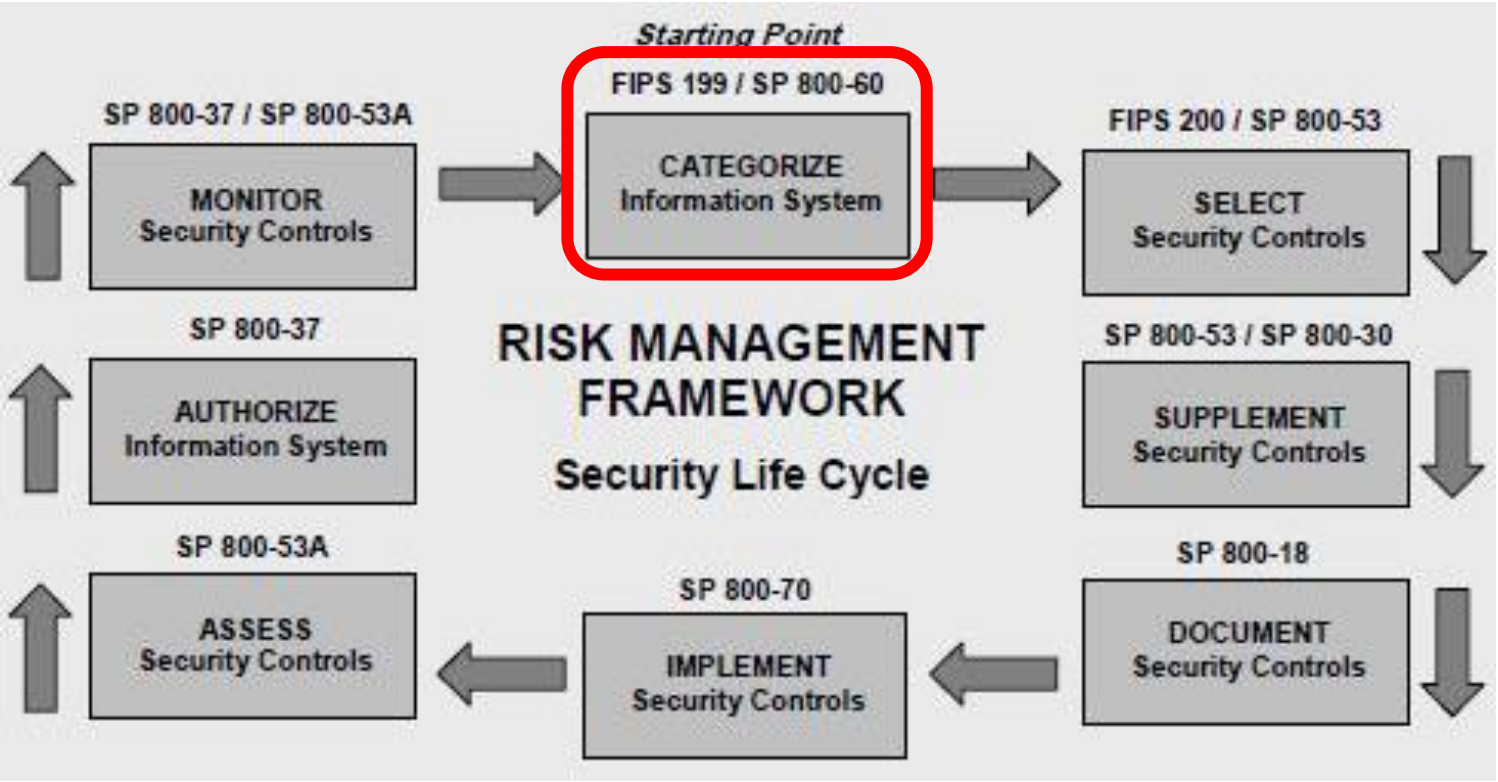
Agenda

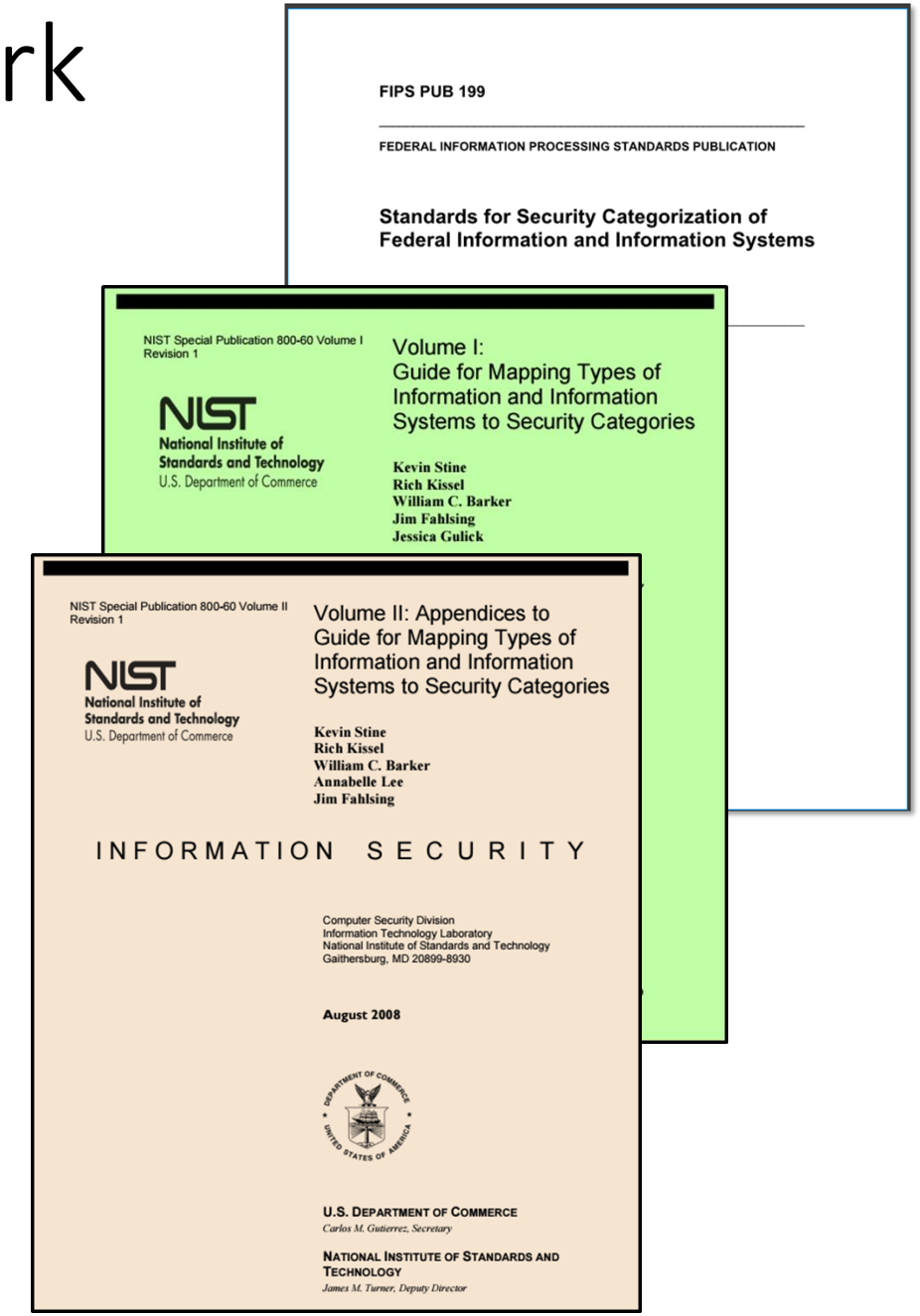
- Risk Management Framework – A quick review…
- Implementing controls – Host hardening…
  - Security configuration checklist (with STIG Viewer)
- SCAP - Security Content Automation Protocol
- System Security Plan’s Appendix 1
  - Select 1 Technical control family to fill out for your information system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

NIST Risk Management Framework



NIST Risk Management Framework





FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

NIST Special Publication 800-60 Volume I
Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

NIST Special Publication 800-60 Volume II
Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Annabelle Lee
Jim Fahlsing

INFORMATION SECURITY

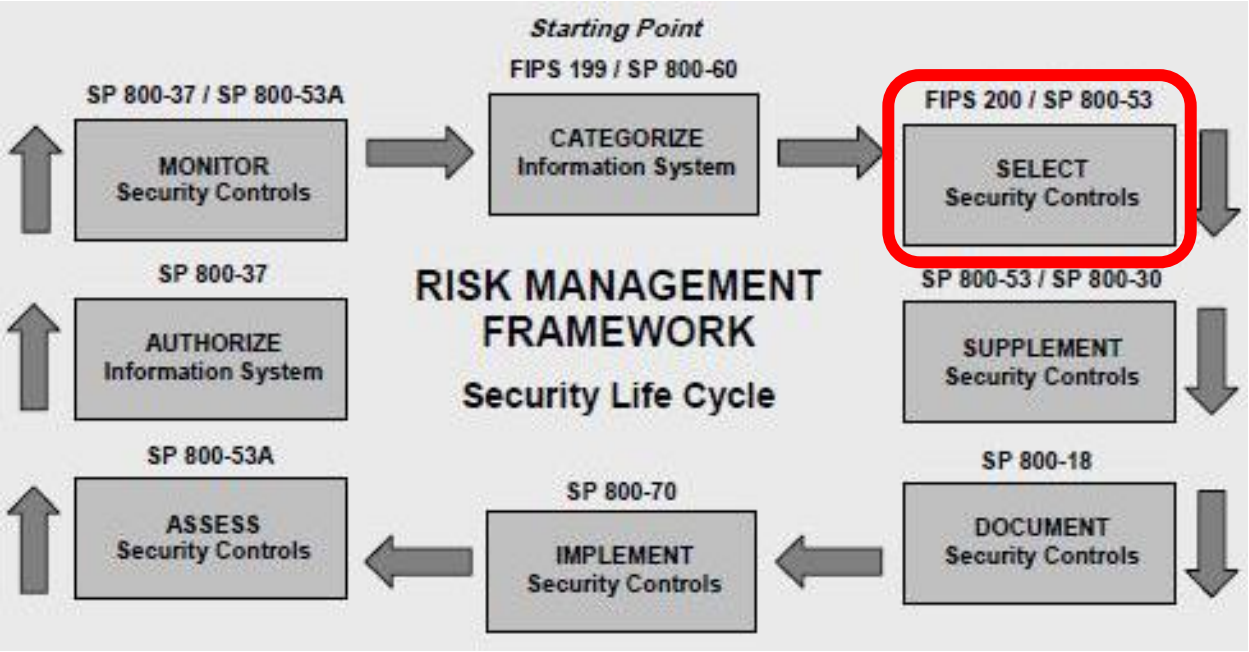
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

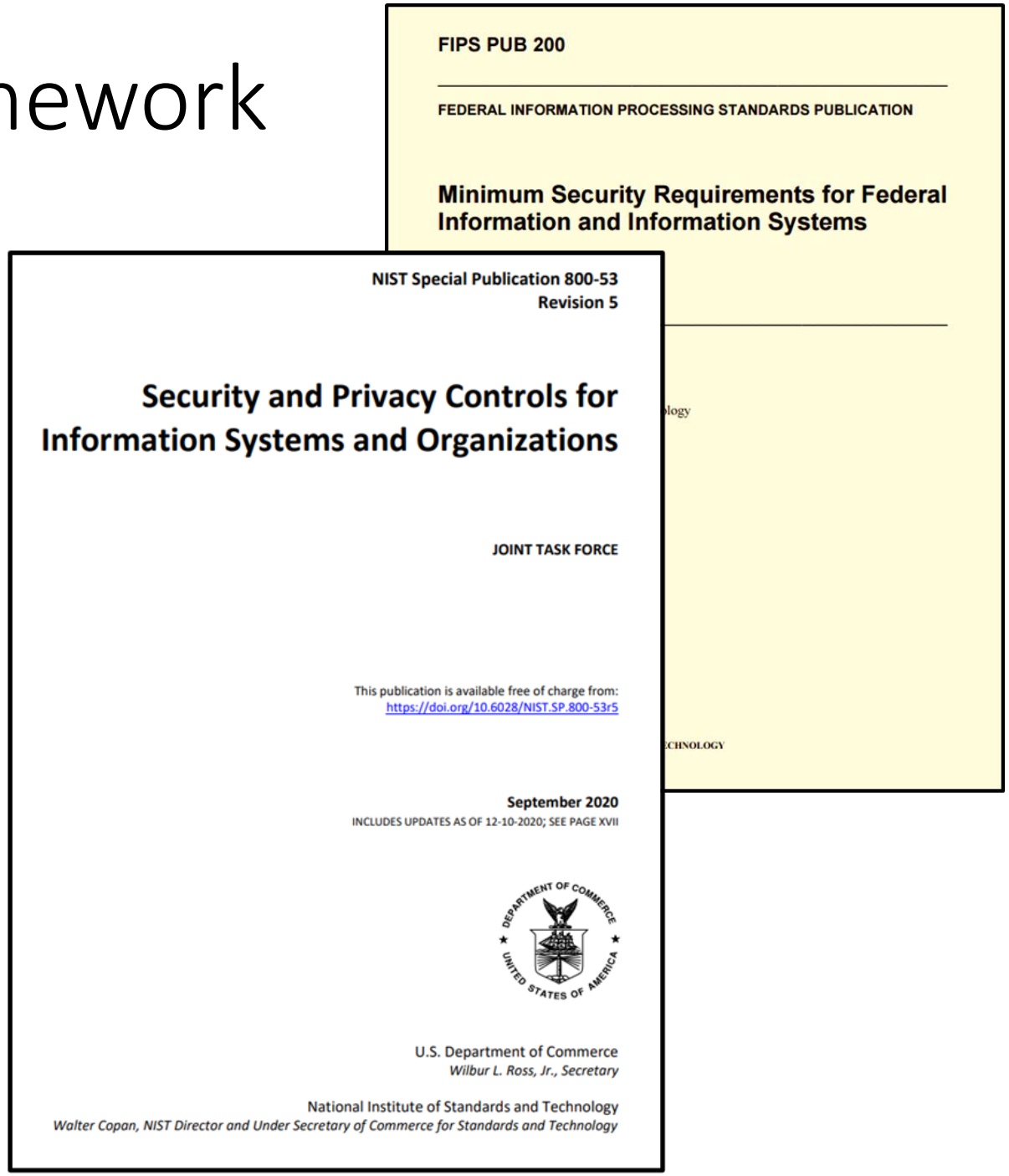
August 2008

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

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
James M. Turner, Deputy Director

NIST Risk Management Framework





FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

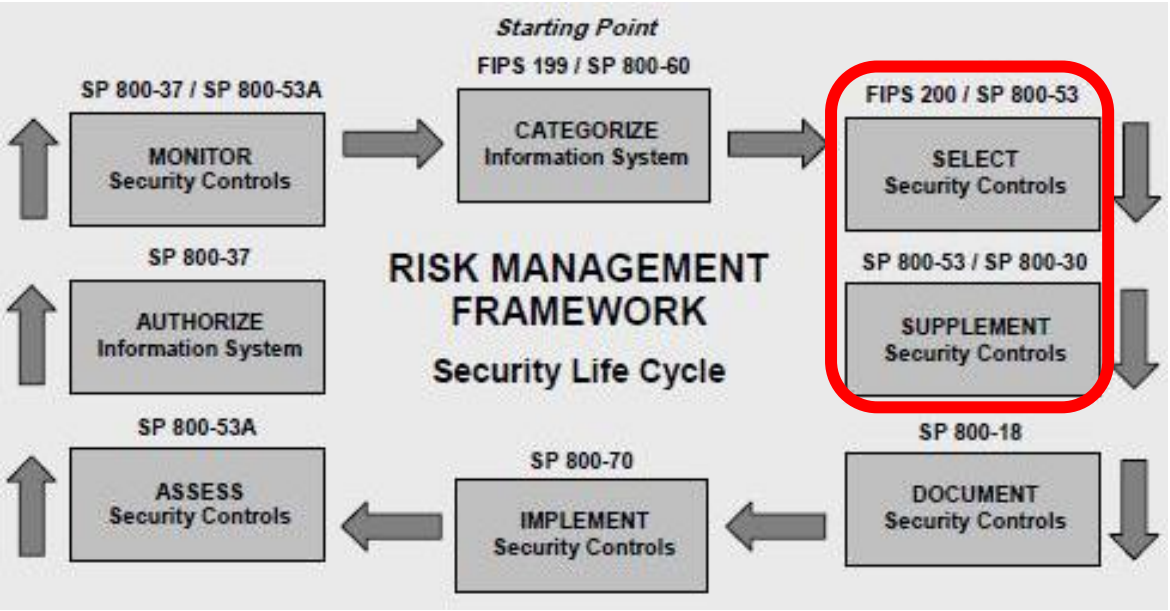
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

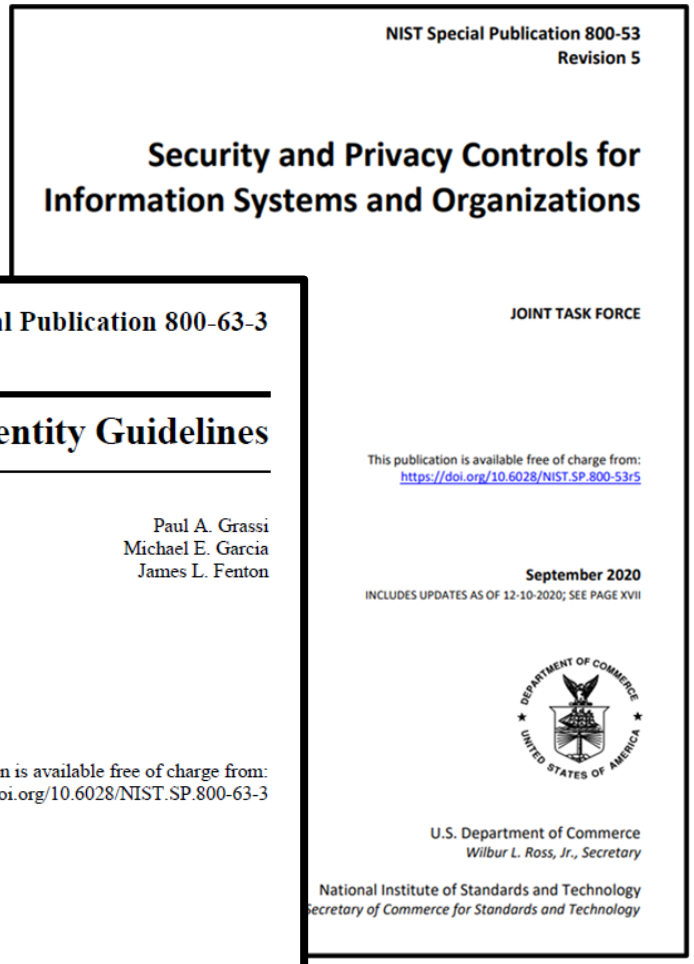
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

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

NIST Risk Management Framework





NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

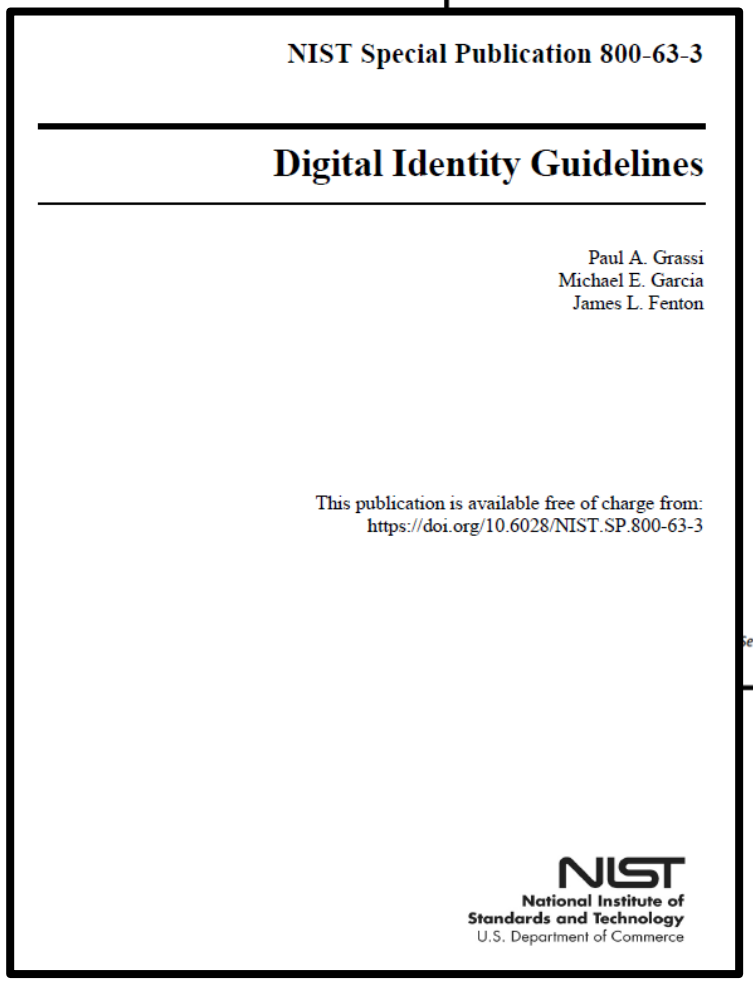
JOINT TASK FORCE

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
Secretary of Commerce for Standards and Technology



NIST Special Publication 800-63-3

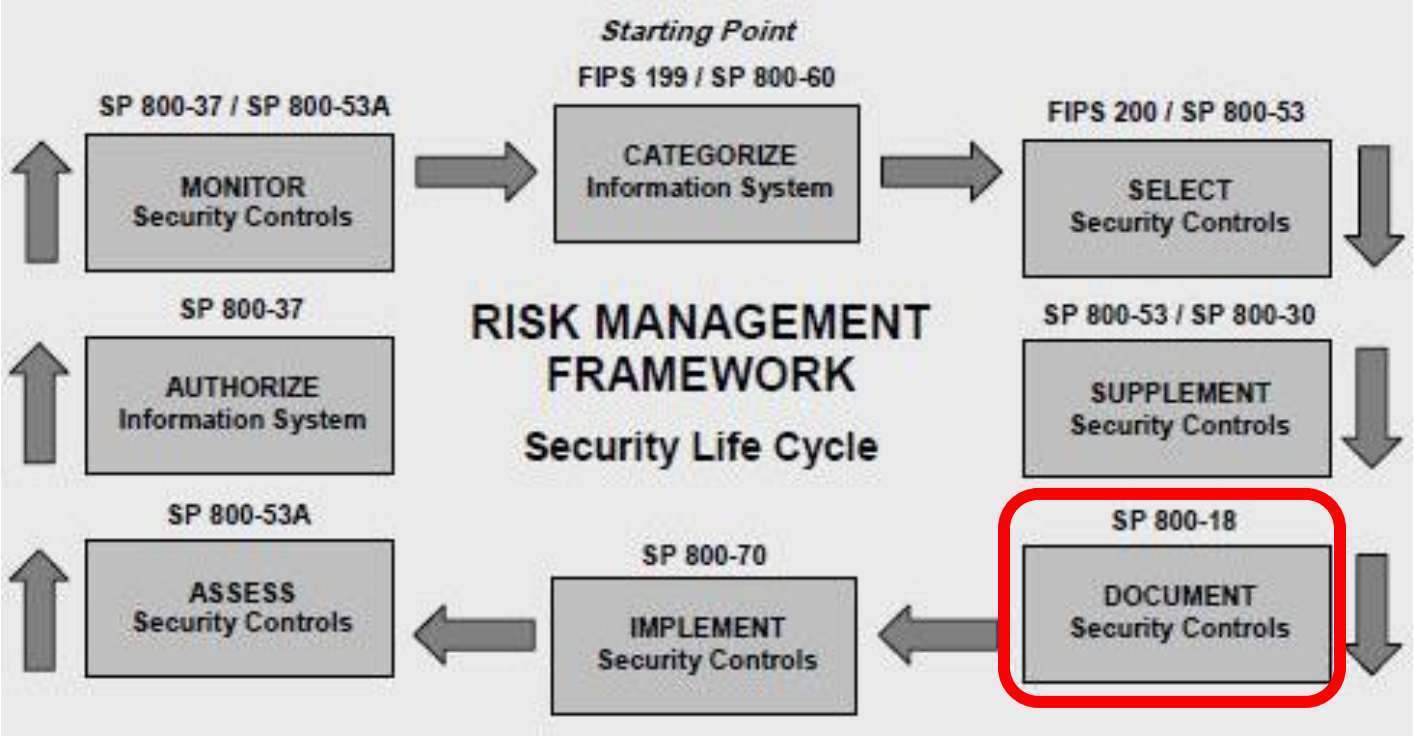
Digital Identity Guidelines

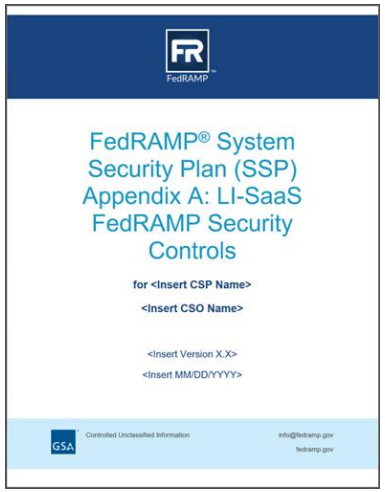
Paul A. Grassi
Michael E. Garcia
James L. Fenton

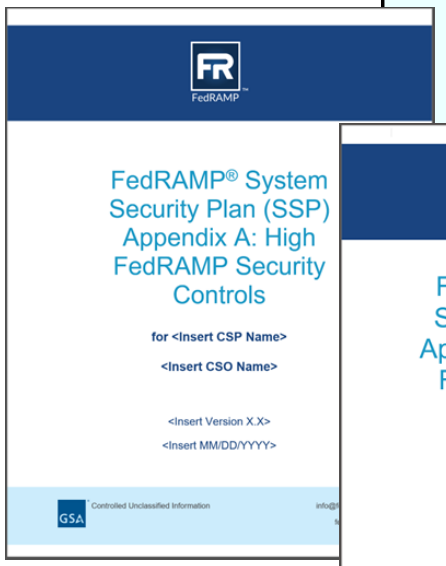
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

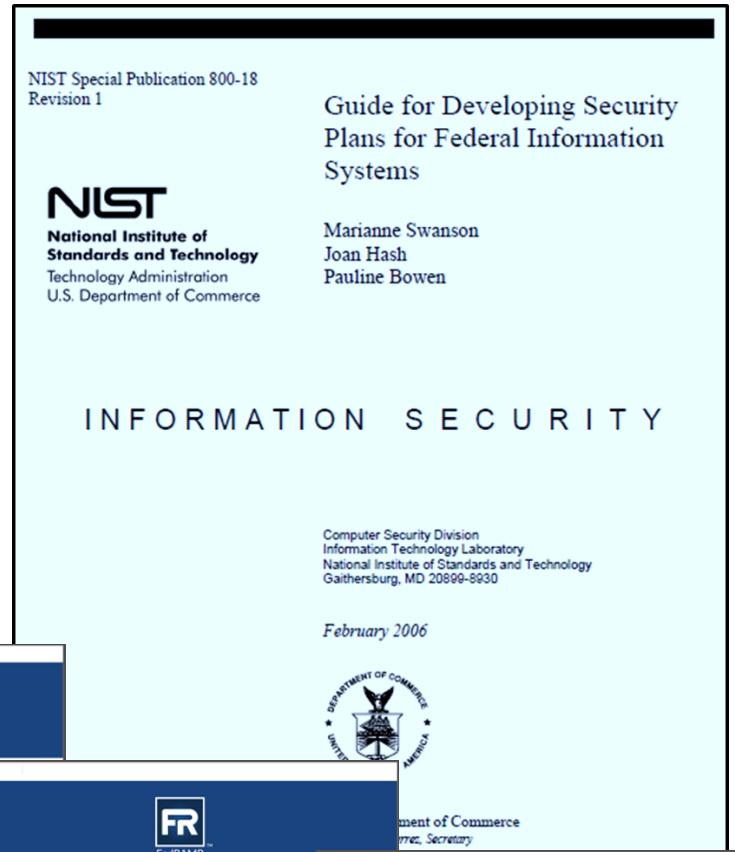
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

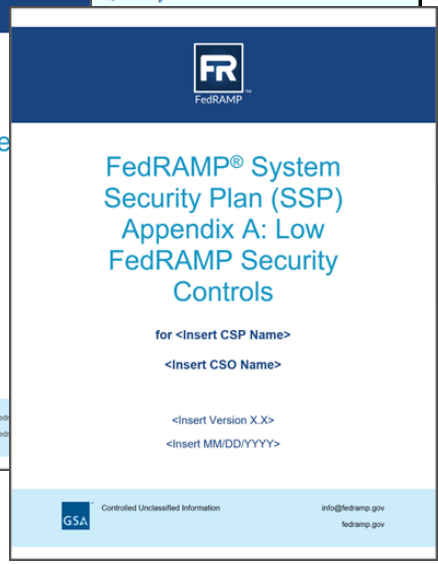
NIST Risk Management Framework



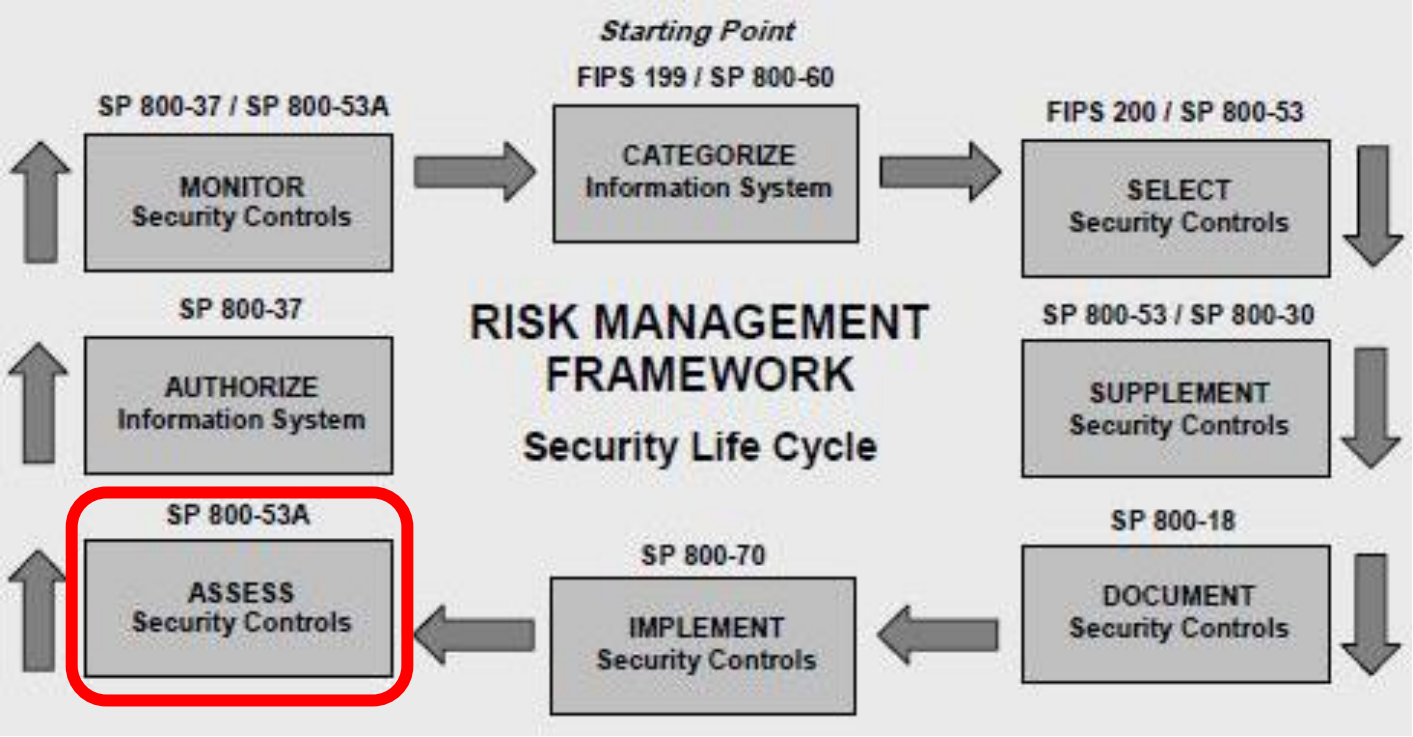




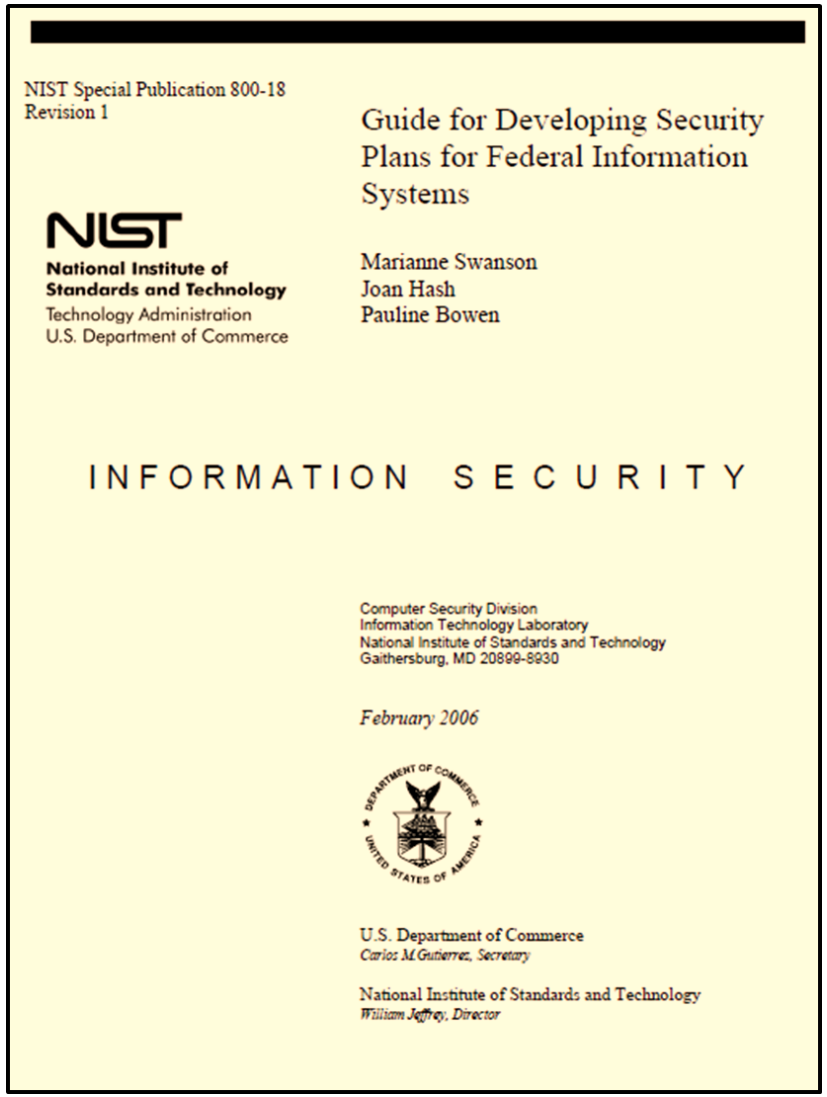




NIST Risk Management Framework



Which controls aid in Host Hardening… ?



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
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. Gutierrez, 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

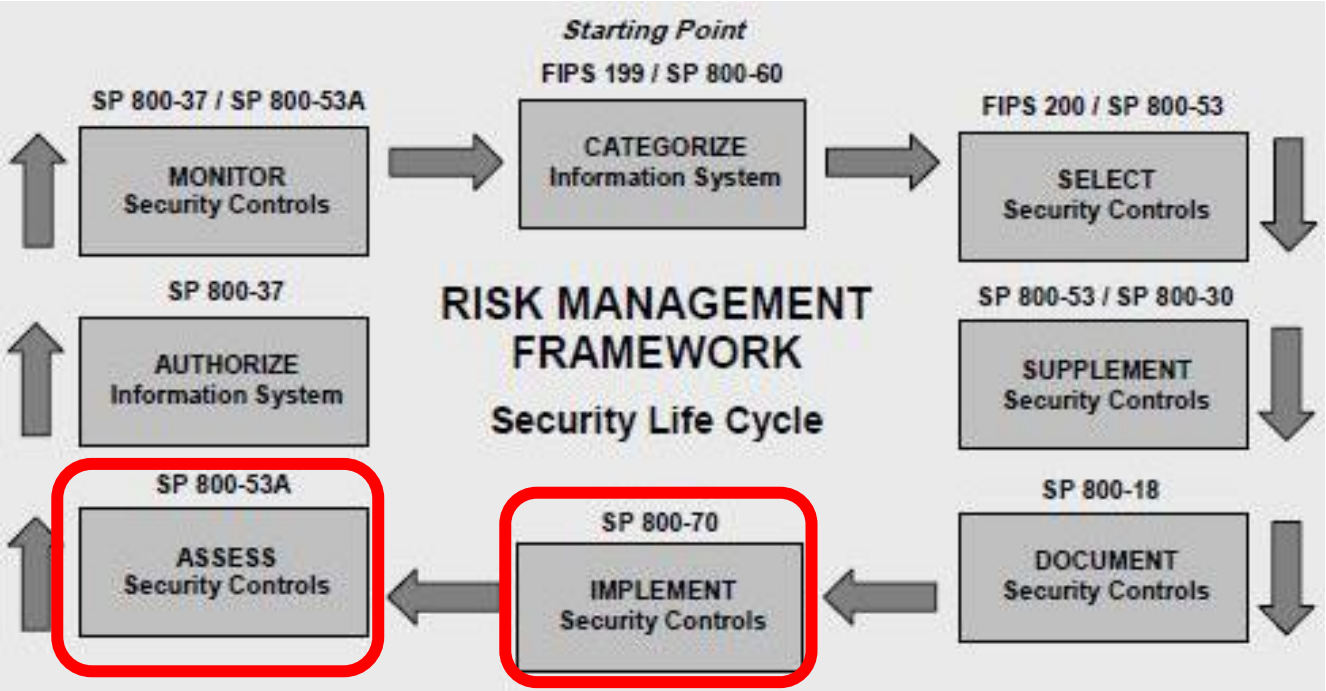
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

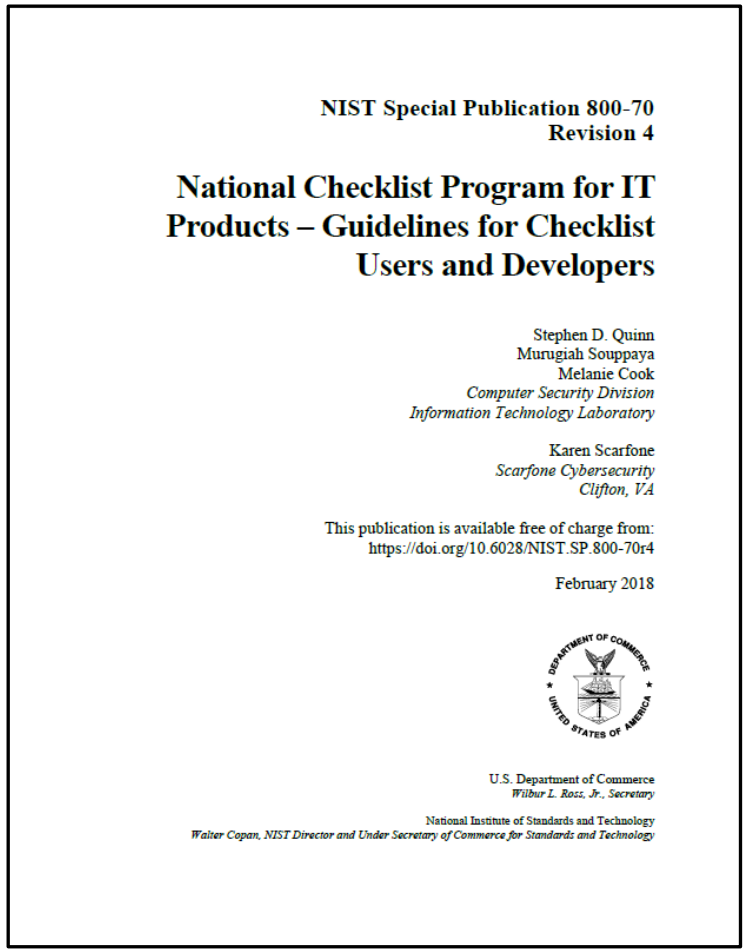
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology
U.S. Department of Commerce

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Configuration Management					
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)





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
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

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:

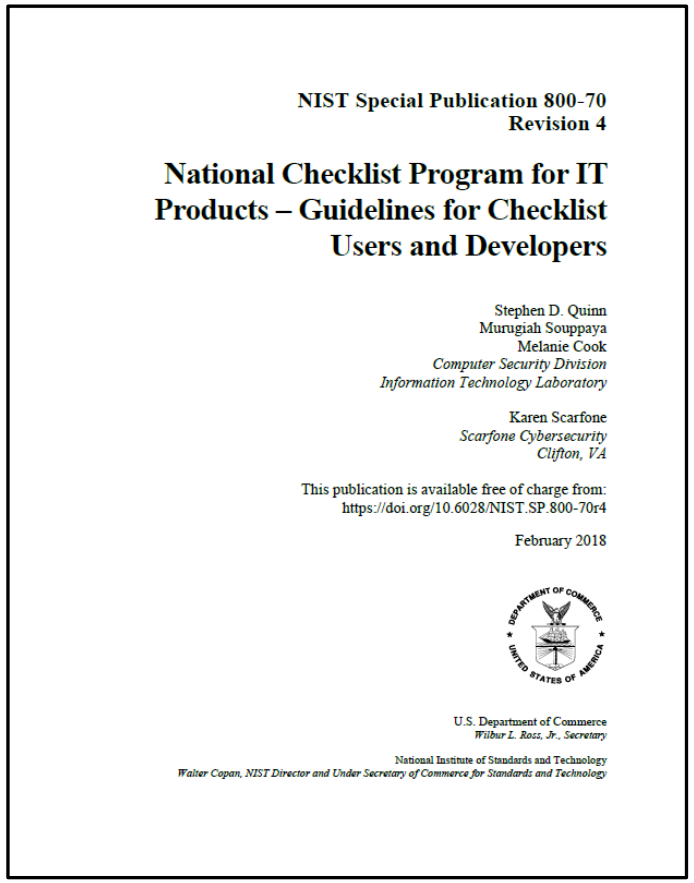
- Minimize the attack surface
- Reduce vulnerabilities
- Lessen the impact of successful attacks
- Identify changes that might otherwise go undetected

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
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

ISACA is a source of many audit control checklists

AUDIT PROGRAM

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

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...

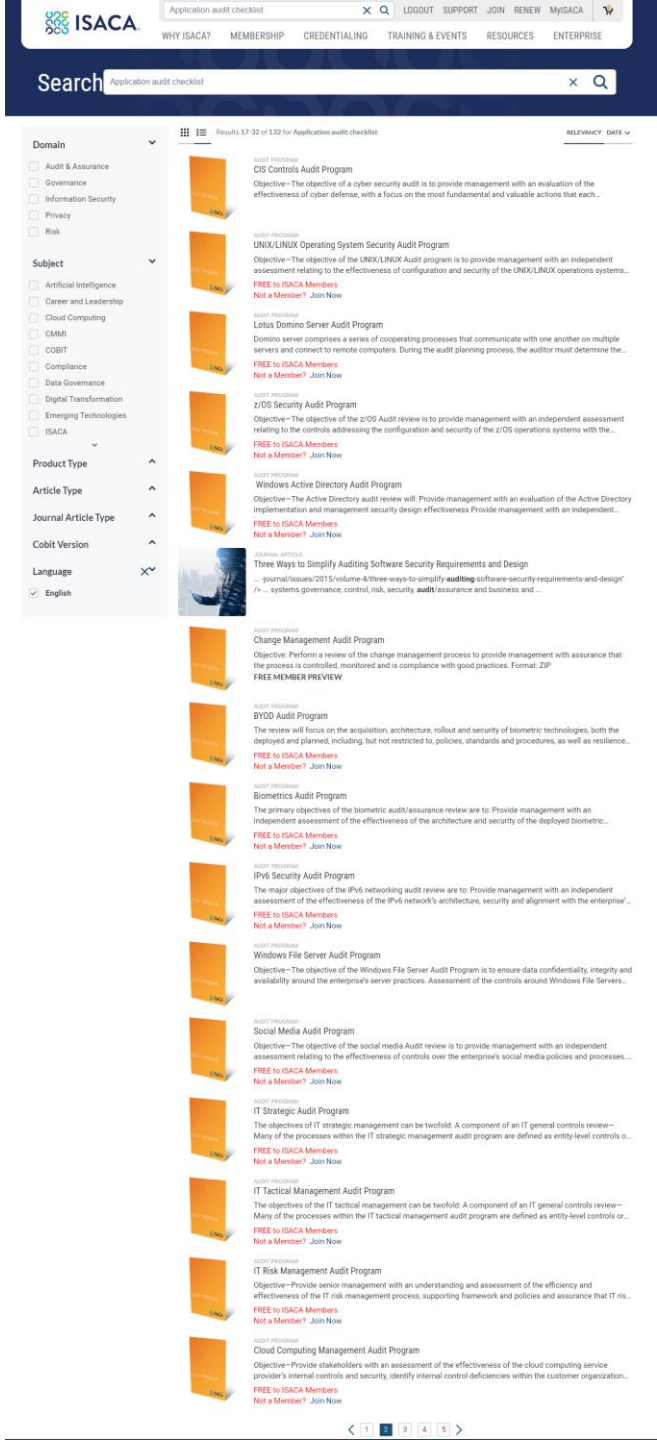
FREE MEMBER PREVIEW

AUDIT PROGRAM

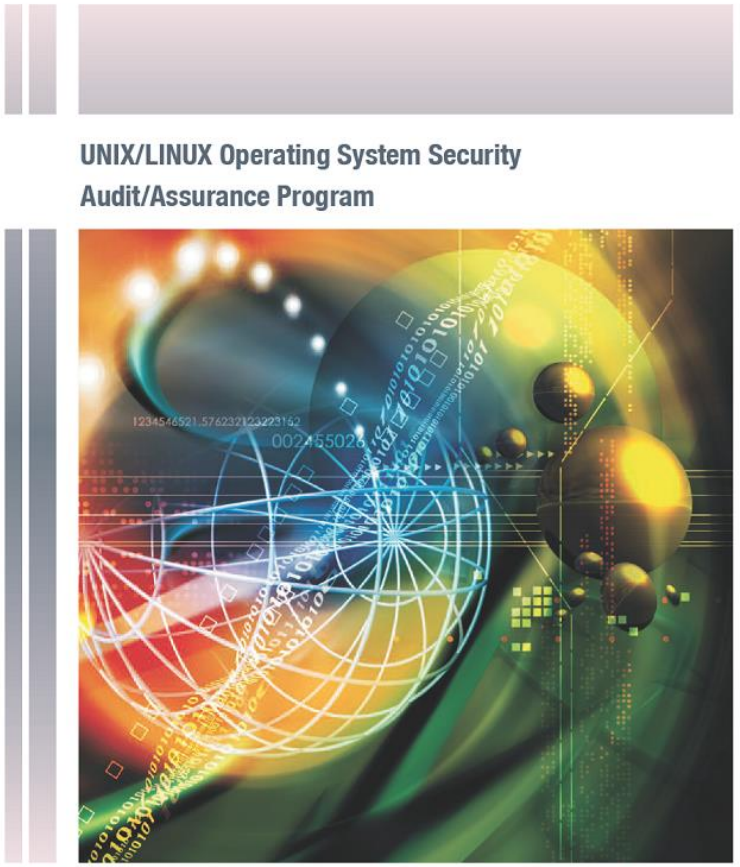
Secure Shell Protocol (SSH) Audit Program

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



UNIX/LINUX Operating System Security Audit Program



Audit Program

Digital materials can be accessed from the Downloaded Materials tab of your *MyISACA* account.

Pages	Date Published	Status
55	2009	Available

Language	Format
English	Digital

UNIX/LINUX Operating System Security Audit/Assurance Program

Table of Contents

effectiveness

tions/functions

Security Technical Implementation Guides

DoD CYBER EXCHANGE PUBLIC

Topics Trai

STIGs Document Library

SECURITY TECHNICAL IMPLEMENTATION GUIDES (STIGS)

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

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

Show 10 entries

Search:

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

Showing 1 to 10 of 548 entries

Previous 1 2 3 4 5 ... 55 Next

STIG TOPICS

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

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

DoD CYBER EXCHANGE PUBLIC

Topics | Training | PKI/PKE | SRGs/STIGs | Resources | Help

- 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
- Help

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.

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

STIG Viewer

STIG Viewer 3.x

TITLE	SIZE	UPDATED
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

DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

STIGs

Filter on STIG name...

CK	Name
☐	A10 Networks ADC ALG Security Technical Implementation Guide
☐	A10 Networks ADC NDM Security Technical Implementation Gui...
☑	Authentication, Authorization, and Accounting Services (AAA) Se...
☐	Active Directory Domain Security Technical Implementation Guide
☐	Active Directory Forest Security Technical Implementation Guide...
☐	Adobe Acrobat Professional DC Continuous Track Security Techn...
☐	Adobe Acrobat Reader DC Continuous Track Security Technical I...
☐	Akamai KSD Service Impact Level 2 ALG Security Technical Imple...
☐	Akamai KSD Service Impact Level 2 NDM Security Technical Impl...
☐	APACHE 2.2 Server for UNIX Security Technical Implementation ...
☐	APACHE 2.2 Site for UNIX Security Technical Implementation Gui...
☐	APACHE 2.2 Server for Windows Security Technical Implementati...

Profile: No Profile

Filter Panel

Must match: All Any

Keyword | Enter filter keyword | Add

Inclusive (+) Filter Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

Remove Filter(s) Remove All Filters

Vul ID	Rule ID	Rule Name
V-80815	SV-95525r1_rule	SRG-APP-0001...
V-80817	SV-95527r1_rule	SRG-APP-0001...
V-80819	SV-95529r1_rule	SRG-APP-0000...
V-80821	SV-95531r1_rule	SRG-APP-0000...
V-80823	SV-95533r1_rule	SRG-APP-0002...
V-80825	SV-95535r1_rule	SRG-APP-0002...
V-80827	SV-95537r1_rule	SRG-APP-0000...
V-80829	SV-95539r1_rule	SRG-APP-0000...
V-80831	SV-95541r1_rule	SRG-APP-0000...
V-80833	SV-95543r1_rule	SRG-APP-0000...
V-80835	SV-95545r1_rule	SRG-APP-0000...
V-80837	SV-95547r1_rule	SRG-APP-0002...
V-80839	SV-95549r1_rule	SRG-APP-0002...
V-80841	SV-95551r1_rule	SRG-APP-0002...
V-80843	SV-95553r1_rule	SRG-APP-0002...
V-80845	SV-95555r1_rule	SRG-APP-0003...
V-80847	SV-95557r1_rule	SRG-APP-0003...
V-80849	SV-95559r1_rule	SRG-APP-0003...
V-80851	SV-95561r1_rule	SRG-APP-0000...
V-80855	SV-95565r1_rule	SRG-APP-0003...
V-80857	SV-95567r1_rule	SRG-APP-0000...
V-80859	SV-95569r1_rule	SRG-APP-0000...
V-80861	SV-95571r1_rule	SRG-APP-0000...
V-80863	SV-95573r1_rule	SRG-APP-0000...
V-80865	SV-95575r1_rule	SRG-APP-0000...
V-80867	SV-95577r1_rule	SRG-APP-0001...
V-80869	SV-95579r1_rule	SRG-APP-0003...
V-80871	SV-95581r2_rule	SRG-APP-0001...
V-80873	SV-95583r1_rule	SRG-APP-0001...
V-80875	SV-95585r1_rule	SRG-APP-0001...
V-80877	SV-95587r1_rule	SRG-APP-0001...
V-80879	SV-95589r1_rule	SRG-APP-0003...
V-80881	SV-95591r1_rule	SRG-APP-0003...

Showing rule 2 out of 164

Authentication, Authorization, and Accounting Services (AAA) Security Requirements Guide :: Version 1, Release: 2
Benchmark Date: 24 Jan 2020

Vul ID: V-80817 **Rule ID**: SV-95527r1_rule **STIG ID**: SRG-APP-000142-AAA-000020

Severity: CAT I **Classification**: Unclass

Group Title: SRG-APP-000142-AAA-000020

Rule Title: AAA Services must be configured to use protocols that encrypt credentials when authenticating clients, as defined in the PPSM CAL and vulnerability assessments.

Discussion: Authentication protection of the client credentials (specifically the password or shared secret) prevents unauthorized 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, can be captured by a third-party. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. Other protocols have similar protections. When unencrypted credentials are passed, adversaries can gain access to resources.

Check Text: Verify AAA Services are configured 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 vulnerability assessments must be reviewed to ensure the protocols are properly configured.

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.

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 vulnerability assessments must be reviewed to ensure the protocols are properly configured.

References

CCI: CCI-000382: The organization configures the information system to prohibit or restrict the use of organization defined functions, ports, protocols, and/or services.
NIST SP 800-53 :: CM-7
NIST SP 800-53A :: CM-7.1 (iii)
NIST SP 800-53 Revision 4 :: CM-7 b

DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

STIGs

Windows

CK	Name
☐	APACHE 2.2 Server for Windows Security Technical Implementati...
☐	APACHE 2.2 Site for Windows Security Technical Implementation...
☐	Apache Server 2.4 Windows Server Security Technical Implement...
☐	Apache Server 2.4 Windows Site Security Technical Implementati...
☐	Citrix Virtual Apps and Desktop 7.x Windows Virtual Delivery Age...
☐	Citrix XenDesktop 7.x Windows Virtual Delivery Agent Security T...
☐	EDB Postgres Advanced Server v11 on Windows Security Technic...
☐	Google Chrome Current Windows Security Technical Implementa...
☐	Microsoft Windows 10 Security Technical Implementation Guide
☑	Microsoft Windows 11 Security Technical Implementation Guide
☐	Microsoft Windows Server 2012/2012 R2 Domain Controller Sec...
☐	Microsoft Windows Server 2012/2012 R2 Member Server Securit...

Profile: No Profile

Filter Panel

Must match: All Any

Keyword | Enter filter keyword | Add

Inclusive (+) Filter Exclusive (-) Filter

+ / -	Keyword	Filter

No content in table

Remove Filter(s) Remove All Filters

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

Showing rule 1 out of 253

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

Vul ID: V-253254 **Rule ID**: SV-253254r828846_rule **STIG ID**: WN11-00-000005

Severity: CAT II **Classification**: Unclass

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

Rule Title: Domain-joined systems must use Windows 11 Enterprise Edition 64-bit version.

Discussion: Features such as Credential Guard use virtualization-based security to protect information that could be used in credential theft attacks if compromised. There are a number of system requirements that must be met in order for Credential Guard to be configured and enabled properly. Virtualization-based security and Credential Guard are only available with Windows 11 Enterprise 64-bit version.

Check Text: Verify domain-joined systems are using Windows 11 Enterprise Edition 64-bit version.

For standalone systems, this is NA.

Open "Settings".

Select "System", then "About".

If "Edition" is not "Windows 11 Enterprise", this is a finding.

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

Fix Text: Use Windows 11 Enterprise 64-bit version for domain-joined systems.

References

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

DISA STIG Viewer : 2.15 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

▼ STIGs

windows 10

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

Profile: No Profile

▼ Filter Panel

Must match: ◉ All ○ Any

CAT I | CAT I | Add

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

+ / -	Keyword	Filter
No content in table		

Remove Filter(s) | Remove All Filters

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

Showing rule 1 out of 257

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

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

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

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

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

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

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

For standalone systems, this is NA.

Open "Settings".

Select "System", then "About".

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

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

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

References

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

DISA STIG Viewer : 2.7

File Export Checklist Options Help

Import STIG

Exit

CK

DISA STIG Viewer : 2.7

File Export Checklist Options Help

STIG Explorer

STIGs

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

CK	Name
	Microsoft O
	Microsoft Po
	Microsoft Pr
	Microsoft Pu
	Microsoft Sh
	Microsoft Vi
	Microsoft W
	Microsoft Ac
	Microsoft Ex
	Microsoft Of
	Microsoft Of
	Microsoft Of
	Microsoft Outlook 2010 Security Technical Implement

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

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

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

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 r*ecommendations* 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

STIG Explorer

STIGs

Filter on STIG name...

CK	Name
	Voice Video Session Management Security Requirements Guide
	vRealize - Cassandra Security Technical Implementation Guide
	Web Policy STIG
	Web Server Security Requirements Guide
	Windows 10 Security Technical Implementation Guide
✓	Windows 10 Security Technical Implementation Guide
	Windows 2008 Domain Controller Security Technical Implementation Guide
	Windows 2008 Domain Controller Security Technical Implementation Guide
	Windows 2008 Member Server Security Technical Implementation Guide
	Windows 2008 Member Server Security Technical Implementation Guide
	Windows 8/8.1 Security Technical Implementation Guide
	Windows Firewall with Advanced Security Security Technical Implementation Guide
	Windows PAW Security Technical Implementation Guide
	Windows PAW Security Technical Implementation Guide

Profile: No Profile

Filter Panel

Must match: All Any

Keyword | Enter filter keyword | Add

Filter Exclusive (-) Filter

+ / -	Keyword	Filter

Keyword
Rule Title
STIG ID
Vulnerability ID
Rule ID
IA Control
CAT I
CAT II
CAT III
CCI

content in table

Remove Filter(s) Remove All Filters

Vul ID	Rule Name
V-63319	WN10-00-000005
V-63321	WN10-CC-000310
V-63323	WN10-00-000010
V-63325	WN10-CC-000315
V-63329	WN10-CC-000320
V-63333	WN10-CC-000325
V-63335	WN10-CC-000330
V-63337	WN10-00-000030
V-63339	WN10-CC-000335
V-63341	WN10-CC-000360
V-63343	WN10-00-000025
V-63345	WN10-00-000035
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63355	WN10-00-000055
V-63357	WN10-00-000060
V-63359	WN10-00-000065
V-63361	WN10-00-000070
V-63363	WN10-00-000075
V-63365	WN10-00-000080
V-63367	WN10-00-000085
V-63369	WN10-CC-000350
V-63371	WN10-00-000090
V-63373	WN10-00-000095
V-63375	WN10-CC-000355
V-63377	WN10-00-000100
V-63381	WN10-00-000105
V-63383	WN10-00-000110
V-63385	WN10-00-000115
V-63403	WN10-00-000140
V-63405	WN10-AC-000005
V-63409	WN10-AC-000010

Showing rule 14 out of 282

Showing rule 14 out of 282

DISA STIG Viewer : 2.9.1 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

STIGs

Filter on STIG name...

CK	Name
	Voice Video Session Management Security Requirements Guide
	vRealize - Cassandra Security Technical Implementation Guide
	Web Policy STIG
	Web Server Security Requirements Guide
	Windows 10 Security Technical Implementation Guide
✓	Windows 10 Security Technical Implementation Guide
	Windows 2008 Domain Controller Security Technical Implementation Guide
	Windows 2008 Domain Controller Security Technical Implementation Guide
	Windows 2008 Member Server Security Technical Implementation Guide
	Windows 2008 Member Server Security Technical Implementation Guide
	Windows 8/8.1 Security Technical Implementation Guide
	Windows Firewall with Advanced Security Security Technical Implementation Guide
	Windows PAW Security Technical Implementation Guide
	Windows PAW Security Technical Implementation Guide

Profile: No Profile

Filter Panel

Must match: All Any

CAT I | CAT I | Add

Inclusive (+) Filter Exclusive (-) Filter

+ / -	Keyword	Filter
+	CAT I	CAT I

Remove Filter(s) Remove All Filters

Vul ID	Rule Name
V-63325	WN10-CC-000315
V-63335	WN10-CC-000330
V-63347	WN10-CC-000345
V-63349	WN10-00-000040
V-63351	WN10-00-000045
V-63353	WN10-00-000050
V-63361	WN10-00-000070
V-63377	WN10-00-000100
V-63429	WN10-AC-000045
V-63651	WN10-CC-000155
V-63667	WN10-CC-000180
V-63671	WN10-CC-000185
V-63673	WN10-CC-000190
V-63739	WN10-SO-000140
V-63745	WN10-SO-000145
V-63749	WN10-SO-000150
V-63759	WN10-SO-000165
V-63797	WN10-SO-000195
V-63801	WN10-SO-000205
V-63847	WN10-UR-000015
V-63859	WN10-UR-000045
V-63869	WN10-UR-000065
V-68845	WN10-00-000145
V-68849	WN10-00-000150
V-78129	WN10-00-000240

Showing rule 4 out of 25

Showing rule 4 out of 25

DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

STIGs

Windo

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

Profile: No Profile

Filter Panel

Must match: All Any

Keyword | Enter filter keyword | Add

Inclusive (+) Filter Exclusive (-) Filter

+ / -	Keyword	Filter
No content in table		

Remove Filter(s) Remove All Filters

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

Showing rule 4 out of 253

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

Vul ID: V-253257 **Rule ID**: SV-253257r828855_rule **STIG ID**: WN11-00-000020

Severity: CAT II **Classification**: Unclass

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: Verify the system firmware is configured for Secure Boot.

For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.

Run "System Information".

Under "System Summary", if "Secure Boot State" does not display "On", this is a finding.

Fix Text: Enable Secure Boot in the system firmware.

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)

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: Verify the system firmware is configured for Secure Boot.

For virtual desktop implementations (VDIs) where the virtual desktop instance is deleted or refreshed upon logoff, this is NA.

Run "System Information".

Under "System Summary", if "Secure Boot State" does not display "On", this is a finding.

Fix Text: Enable Secure Boot in the system firmware.

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)

system information app

	Value
	Microsoft Windows 11 Pro
	10.0.22621 Build 22621
on	Not Available
	Microsoft Corporation
	MIS-DLANTER-X1E
er	LENOVO
	20Y5007QUS
	x64-based PC
	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...
	LENOVO N40ET37W (1.19), 8/26/2022
	3.2
ler Version	1.16
	UEFI
cturer	LENOVO
	20Y5007QUS
	SDK0T76530 WIN
Platform Role	Mobile
Secure Boot State	Off
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\WINDOWS
System Directory	C:\WINDOWS\system32
Boot Device	\Device\HarddiskVolume1
Locale	United States
Hardware Abstraction Layer	Version = "10.0.22621.1413"
User Name	MIS-DLanter-X1E\David Lanter
Time Zone	Eastern Daylight Time
Installed Physical Memory (RAM)	32.0 GB
Total Physical Memory	31.7 GB
Available Physical Memory	15.8 GB
Total Virtual Memory	33.7 GB
Available Virtual Memory	13.0 GB
Page File Space	2.00 GB
Page File	C:\pagefile.sys
Kernel DMA Protection	On
Virtualization-based security	Running

Find what: Find Close Find

Search selected category only Search category names only

Showing rule 4 out of 253

system Information

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)

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

SC-08(01)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	SC-08(01)_ODP	***one or more of the following PARAMETER VALUES is/are selected: {prevent unauthorized disclosure of information; detect changes to information};***
	SC-08(01)	cryptographic mechanisms are implemented to ***<SC-08(01)_ODP SELECTED PARAMETER VALUE(S)>*** during transmission.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	SC-08(01)-Examine	[SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality and integrity; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; other relevant documents or records].
	SC-08(01)-Interview	[SELECT FROM: System/network administrators; organizational personnel with information security responsibilities; system developer].
	SC-08(01)-Test	[SELECT FROM: Cryptographic mechanisms supporting and/or implementing transmission confidentiality and/or integrity; mechanisms supporting and/or implementing alternative physical safeguards; organizational processes for defining and implementing alternative physical safeguards].

DISA STIG Viewer : 2.17 : STIG Explorer

File Export Checklist Options Help

STIG Explorer

STIGs

Windo

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

Profile: No Profile

Filter Panel

Must match: All Any

Keyword | Enter filter keyword | Add

Inclusive (+) Filter Exclusive (-) Filter

+ / -	Keyword	Filter
No content in table		

Remove Filter(s) Remove All Filters

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

Showing rule 6 out of 253

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

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

Severity: CAT II **Classification**: Unclass

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

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

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

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

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

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

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

Open "BitLocker Drive Encryption" from the Control Panel.

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

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

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

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

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

References

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

Group Title: WN10-00-000030

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

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

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

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

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

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

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

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

Control Panel › System and Security ›

Search Control Panel

Control Panel Home

System and Security

Network and Internet

Hardware and Sound

Programs

User Accour

Appearance

Personalization

Clock and Region

Ease of Access

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

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

Power Options
Change battery settings | Change what the power bu

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

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

BitLocker Drive Encryption
Manage BitLocker

BitLocker Drive Encry
Protect your PC usin
Encryption.

Storage Spaces
Manage Storage Spaces

Work Folders
Manage Work Folders

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

control panel **open**

control panel **windows 10**

control panel **settings**

control panel **home**

Uninstall a

Control Panel › System and Security › BitLocker Drive Encryption

Search Con

Control Panel Home

BitLocker Drive Encryption

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

Operating system drive

Windows (C:) BitLocker off

Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

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

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)

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

Show 10 entries Search:

TITLE	SIZE	UPDATED
Adobe Acrobat Reader DC Continuous Track STIG Benchmark - Ver 2, Rel 2	10.86 KB	21 Oct 2022
Canonical Ubuntu 18.04 LTS STIG Benchmark - Ver 2, Rel 8	62.01 KB	13 Jan 2023
Canonical Ubuntu 20.04 LTS STIG Benchmark - Ver 1, Rel 5	61.15 KB	13 Jan 2023
Google Chrome STIG Benchmark - Ver 2, Rel 8	24.25 KB	13 Jan 2023
Microsoft .NET Framework 4 STIG Benchmark - Ver 2, Rel 2	7.51 KB	13 Jan 2023
Microsoft Defender Antivirus STIG Benchmark - Ver 2, Rel 3	23.2 KB	25 May 2022
Microsoft Edge STIG Benchmark - Ver 1, Rel 2	1.53 MB	27 Oct 2022
Microsoft Internet Explorer 11 STIG Benchmark - Ver 2, Rel 4	66.02 KB	13 Jan 2023
Microsoft Windows 10 STIG Benchmark - Ver 2, Rel 7	100.42 KB	13 Jan 2023
Microsoft Windows 11 STIG Benchmark - Ver 1, Rel 1	94.76 KB	17 Nov 2022

Showing 1 to 10 of 26 entries

Previous 1 2 3 Next

SCAP TOOLS

tenable.sc Dashboard Analysis Scans Reporting Assets Workflow Users

SCAP Audit Summary

Switch Dashboard Options

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
1036177	CCE-26741-9::SV-50459r5_rule:RHEL_6_STIG_001.017:MAC-1_Classified	High	1

Last Updated: Less than a minute ago

SCAP Audit Summary - Top 25 Windows Compliance Failed Checks

Plugin ID	Name	Severity	Total
1035021	CCE-43078-5::SV-78115r1_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4
1035018	CCE-42970-4::SV-78109r1_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4
1035012	CCE-43470-4::SV-78091r1_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4
1034963	CCE-42218-8::SV-77923r2_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4
1034959	CCE-42218-8::SV-77915r2_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4
1034952	CCE-42187-5::SV-77901r2_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4
1034950	CCE-42073-7::SV-77897r2_rule:Windows_10_STIG_001.007:MAC-1_Classified	High	4

Common Configuration Enumeration (CCE) The CCE List provides unique identifiers to security-related system configuration issues

SCAP Audit Summary - Compliance Summary

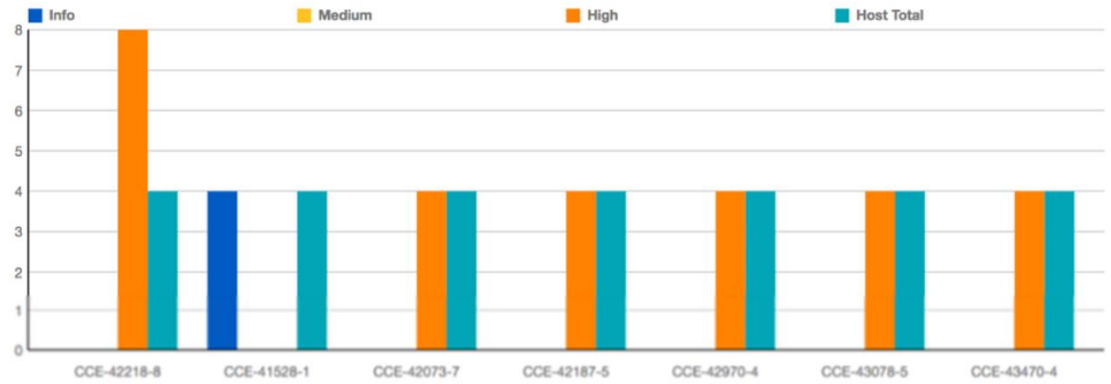
	Systems	Passed	Manual Check	Failed
Windows	4	13%	0%	88%
Linux	1	57%	0%	43%

Last Updated: Less than a minute ago

SCAP Audit Summary - Network Summary

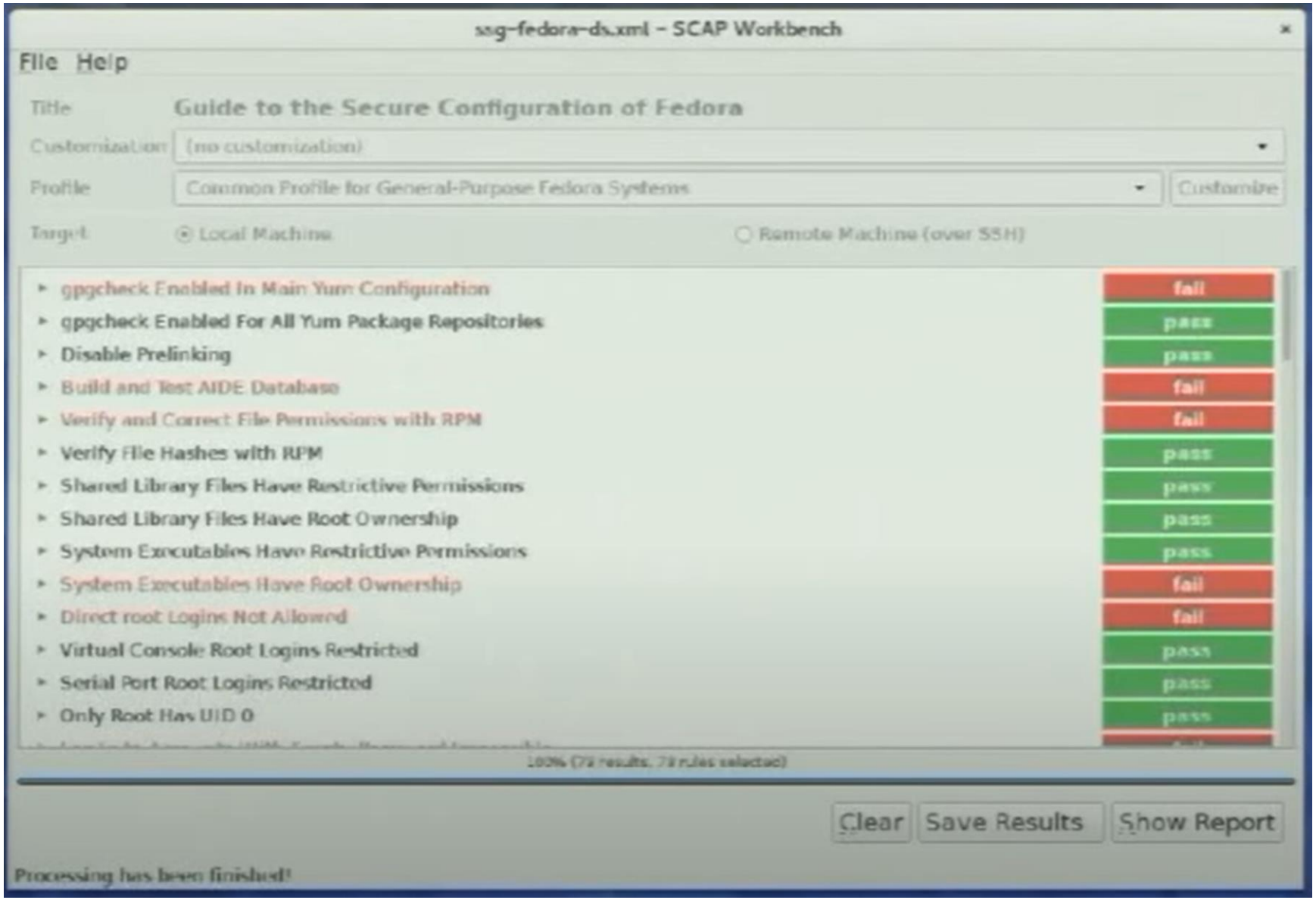
IP Address	Score	Info	Medium	High	Total
[illegible]	750	99	0	75	174
[illegible]	210	3	0	21	24
[illegible]	70	1	0	7	8

SCAP Audit Summary - Top 10 CCE



Last Updated: 3 minutes ago

SCAP Compliance Scan Results



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

FAILED CCE-10103-0:Always prompt client for password upon connection

Description

Always prompt client for password upon connection

The "Always Prompt Client for Password upon Connection" policy should be set correctly for Terminal Services.

Audit File

Win7-510-1.2.7.1.zip

Policy Value

xccdf_gov.nist_rule_always_prompt_for_password_upon_connection: PASSED

Output

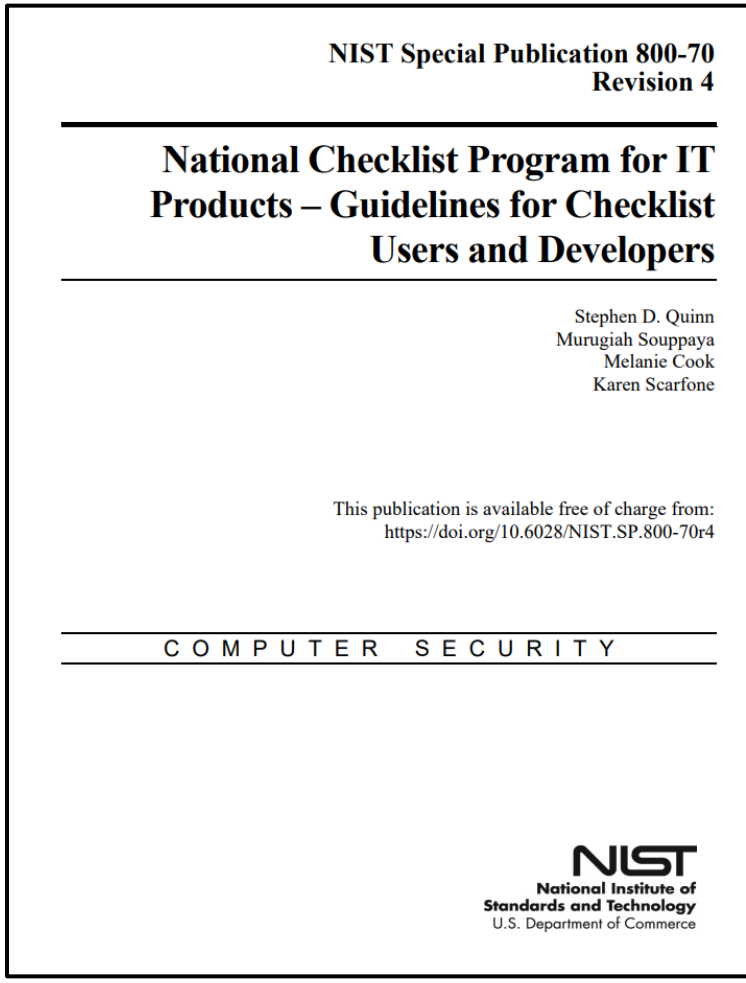
```
xccdf_gov.nist_rule_always_prompt_for_password_upon_connection: FAILED
```

Reference Information

UPDATED-DATE: 2012-02-24T10:00:00
RULE-ID: xccdf_gov.nist_benchmark_USGCB-Windows-7:xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1:xccdf_gov.nist_rule_always_prompt_for_password_upon_connection
GENERATED-DATE: 2012-02-24T10:00:00
SCAN-DATE: 2014-11-11T16:53:40
OVAL-DEF: oval:gov.nist.usgcb.windowsseven:def:275
CCE: CCE-10103-0
SEVERITY: unknown

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

- National Vulnerability Database (NVD): https://nvd.nist.gov/
- NVD SCAP Download: http://nvd.nist.gov/download.cfm
- National Checklist Program (NCP): http://web.nvd.nist.gov/view/ncp/repository
- 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

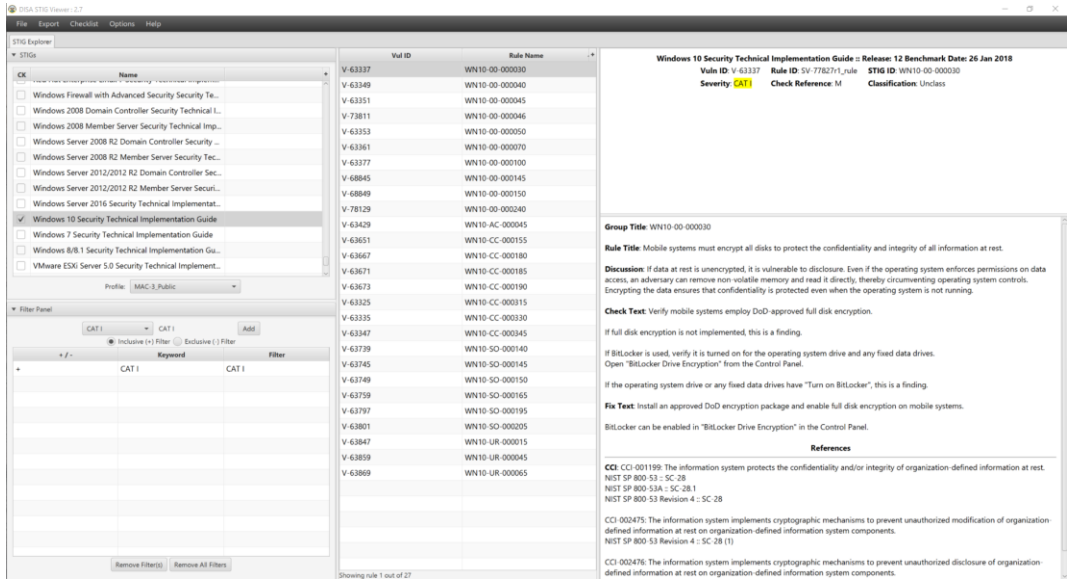
COMPUTER SECURITY

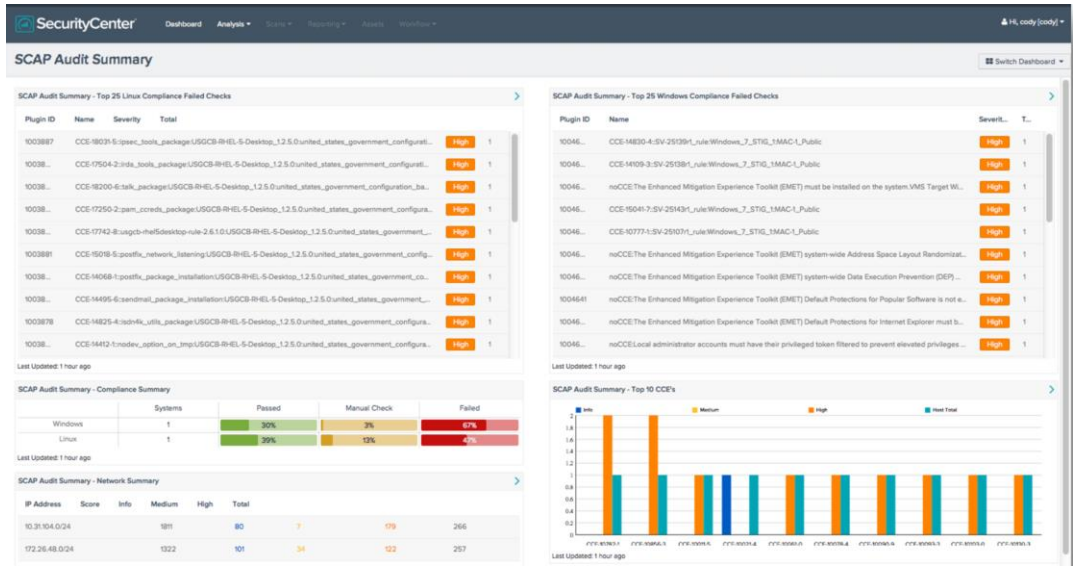
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DISA STIG Tool

+

SCAP Tool





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.

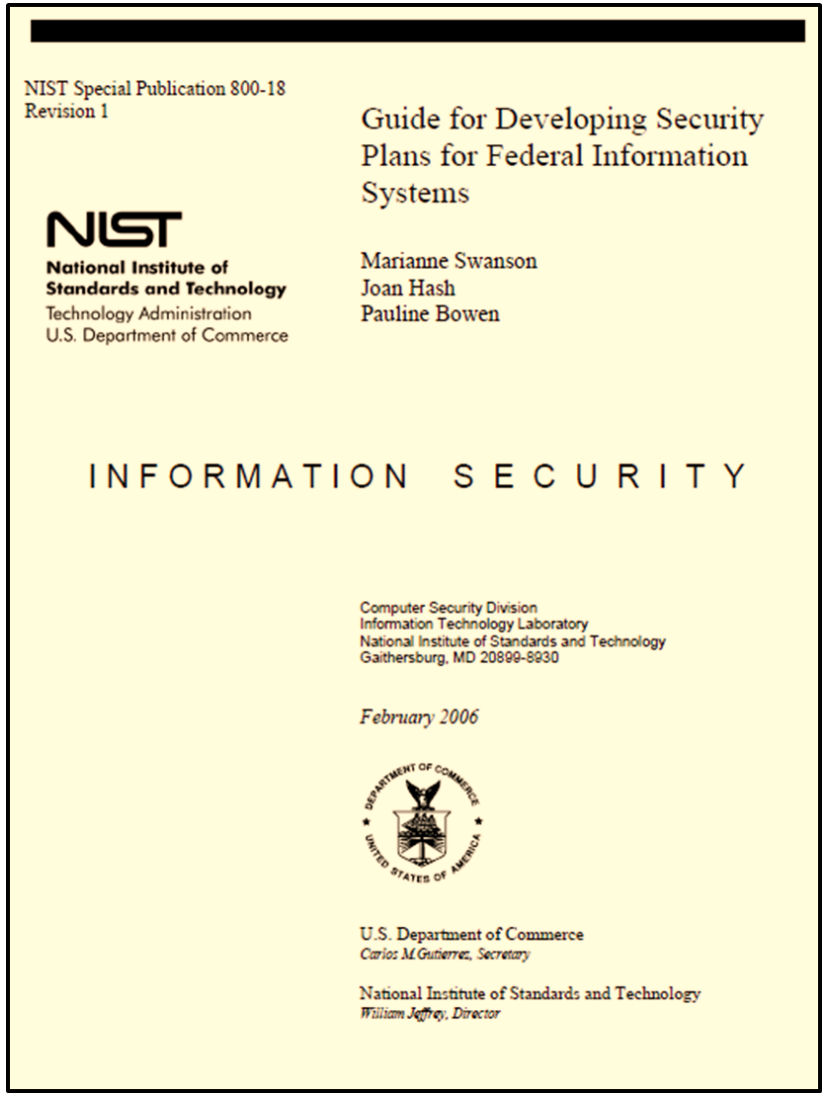
Agenda

- ✓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

SSP’s Technical Controls: SSP’s Appendix A



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
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

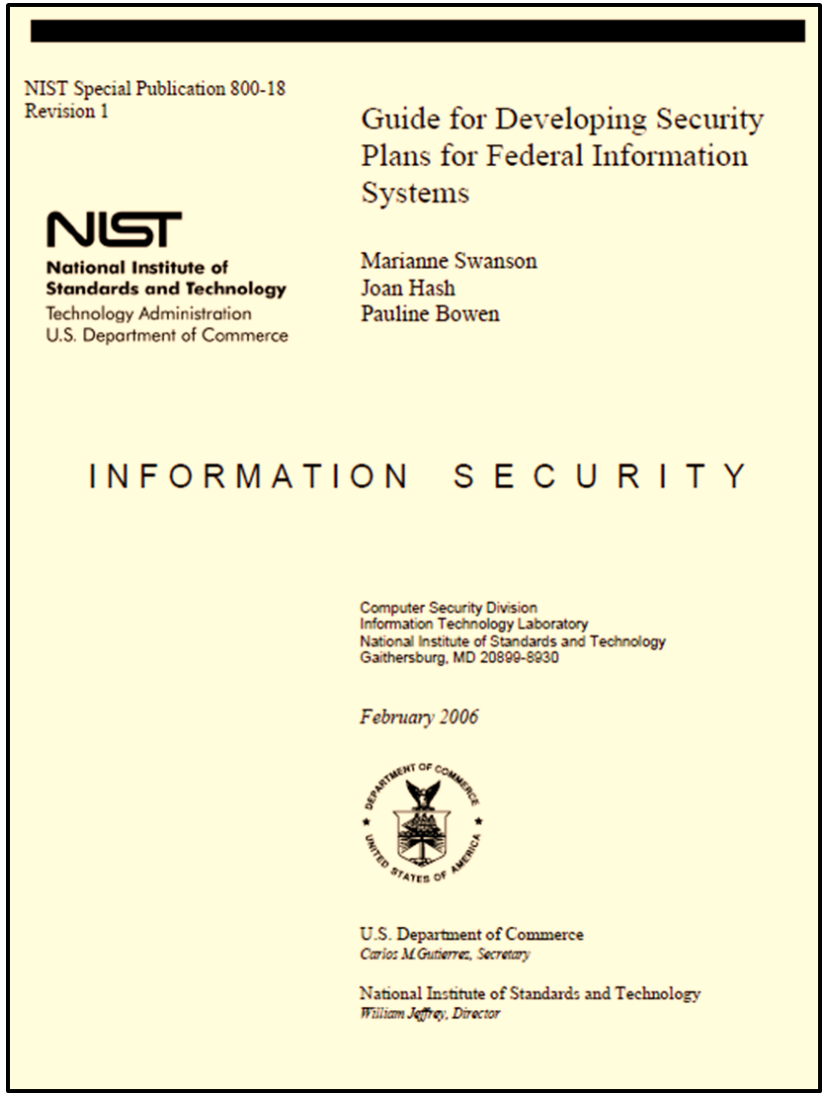
U.S. Department of Commerce
Carlos M Gutierrez, Secretary

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

Technical Controls



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
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

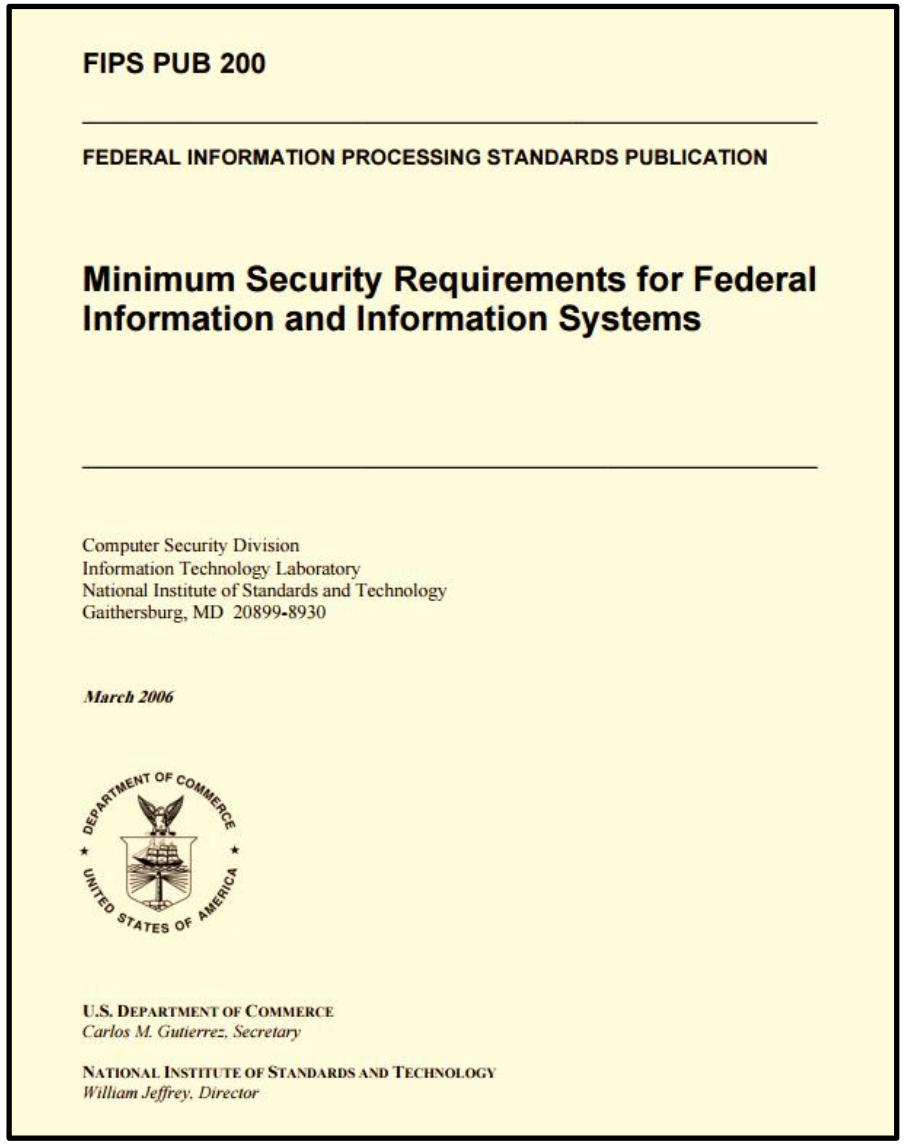
U.S. Department of Commerce
Carlos M Gutierrez, Secretary

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

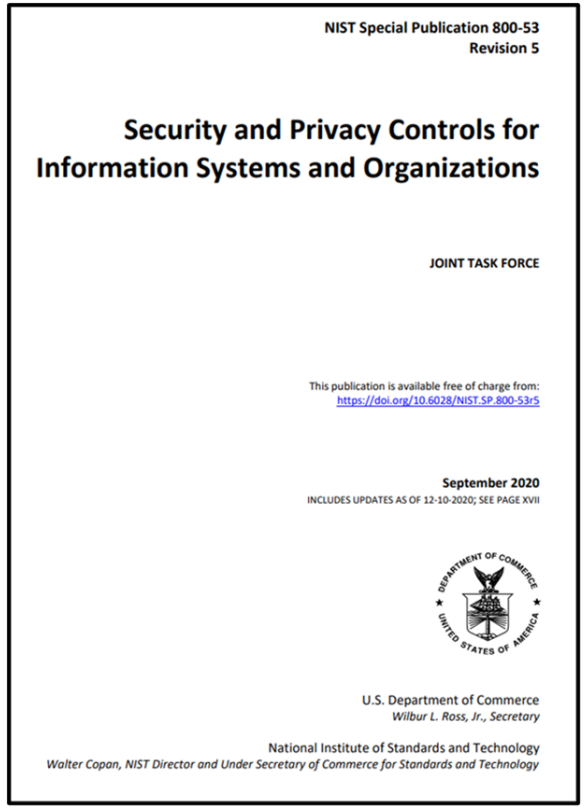
info@fedramp.gov

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/YYYY>

Identification and Authentication (IA)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Identification and Authentication					
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-1 Identification and Authentication Policy and Procedures

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

a. Develops, documents, and disseminates to **[*Assignment: organization-defined 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*]**.

IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES			
	ASSESSMENT OBJECTIVE: *Determine if the organization:*			
	IA-1(a)(1)	IA-1(a)(1)[1]	*develops and documents an identification and authentication policy that addresses:*	
			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]	*defines personnel or roles to whom the identification and authentication 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]	*defines the frequency to review and update the current identification and authentication policy;*	
		IA-1(b)(1)[2]	*reviews and updates the current identification and authentication 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]	*reviews and updates the current identification and authentication procedures with the organization-defined frequency.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Identification and authentication policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with identification and authentication responsibilities; organizational personnel with information security responsibilities].			

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

IA-1 Identification and Authentication Policy and Procedures

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

James L. Fenton
Altmode Networks
Los Altos, Calif.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017
INCLUDES UPDATES AS OF 12-01-2017; PAGE X

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

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

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.

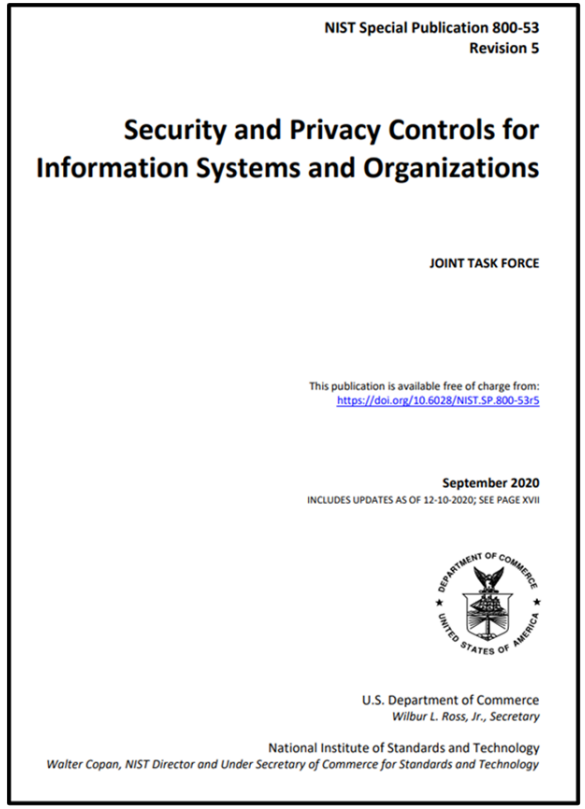
Examples of Level I (low sensitivity) institutional data:

- 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 NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Identification and Authentication					
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

A-2 *is a common control to all baselines*

IA-2 Identification and Authentication (Organizational Users)

Control: 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

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 CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
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

	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	Information Type	Inconvenience, distress or damage to standing or reputation	Financial loss or agency liability	Harm to agency programs or public interests	Unauthorized release of sensitive information	Personal Safety	Civil or criminal violations	IAL	AAL
Environmental Management	D.8	Pollution Prevention and Control	Low	Low	Low	Low	Low	Low	2	2
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		
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

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 NIST SP 800-63 Digital Identity Guidelines 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

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>

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

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>

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	☐

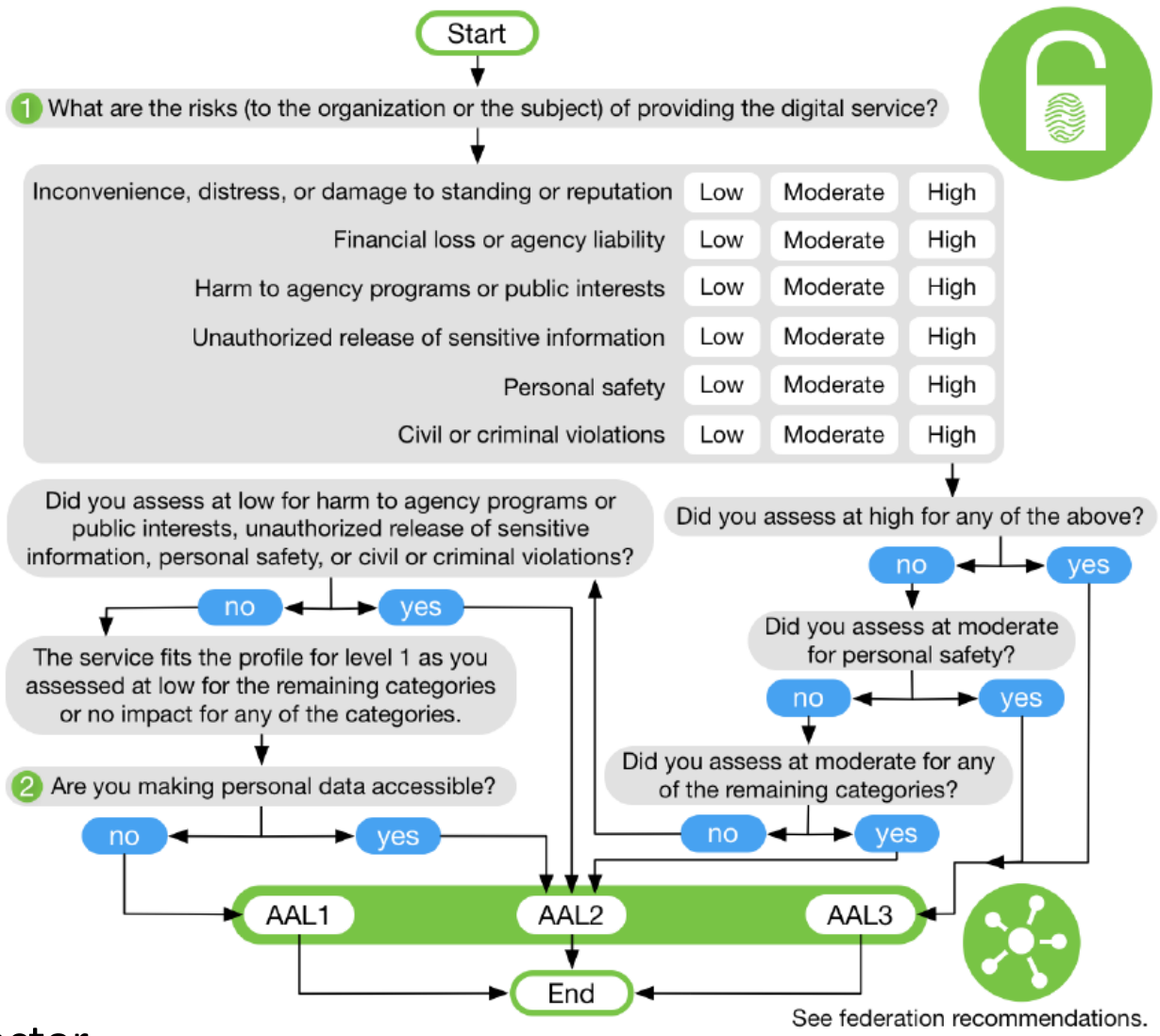
IA-2 Identification and Authentication

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].

Authenticator Assurance

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
Verifier-Compromise Resistance	Not required	Not required	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



AAL1 : = 1 Factor

AAL2 : = 2 Factors

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

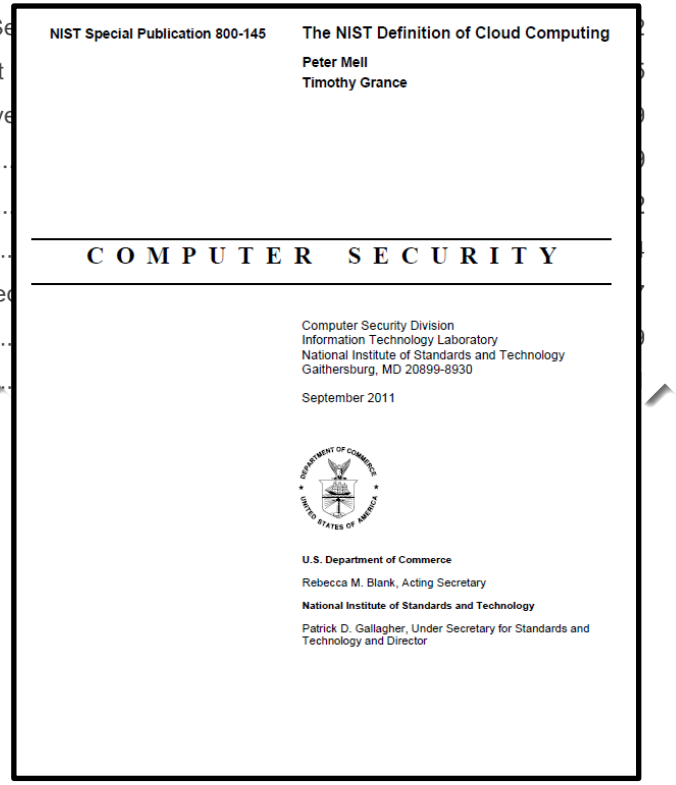
AAL = Authenticator Assurance Level

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



NIST Special Publication 800-145

The NIST Definition of Cloud Computing

Peter Mell
Timothy Grance

COMPUTER SECURITY

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

September 2011

U.S. Department of Commerce

Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology

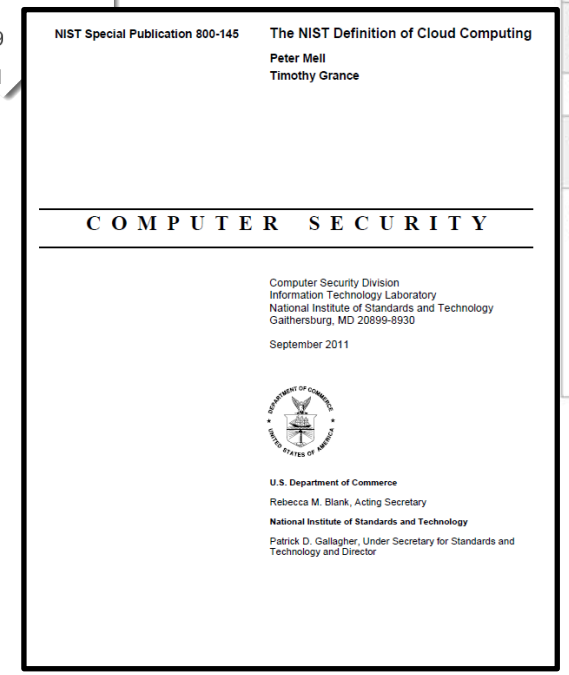
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

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 CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
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.)].

TABLE OF CONTENTS



NIST Special Publication 800-145

The NIST Definition of Cloud Computing

Peter Mell
Timothy Grance

COMPUTER SECURITY

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

September 2011

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

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>

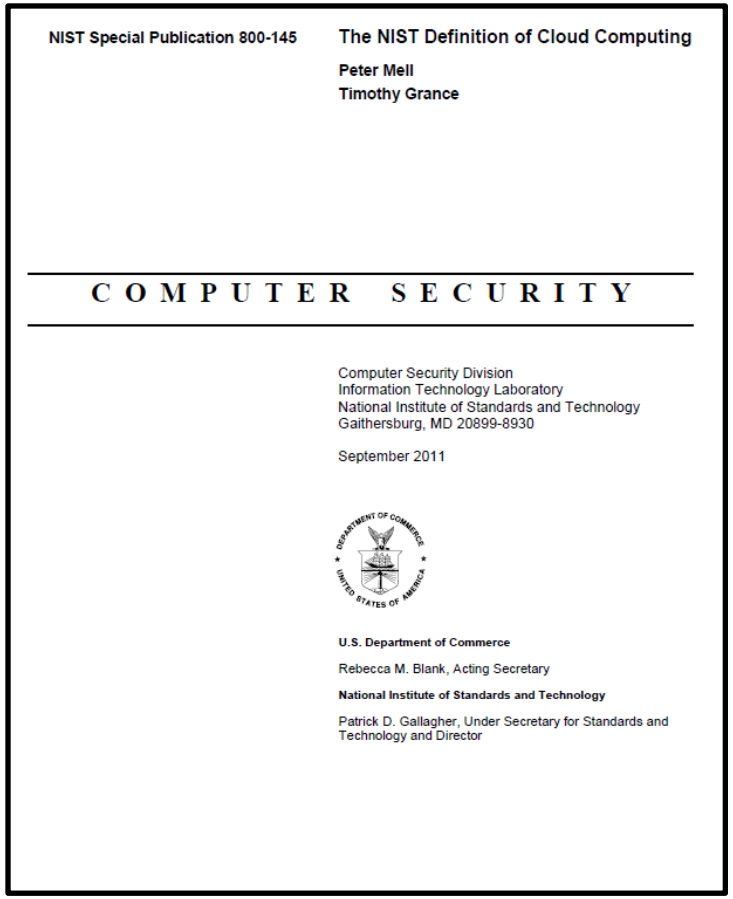
Table 3.1 provides a summary of the key attributes of the CSO.

Table 3.1 System Information

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
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.)].

Essential Characteristics of Cloud Computing

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



NIST Special Publication 800-145

The NIST Definition of Cloud Computing

Peter Mell
Timothy Grance

COMPUTER SECURITY

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

September 2011

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

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 exclusive use by a single organization 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 exclusive use by a specific community of consumers from 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 composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, 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

System Information	
CSP Name:	<Insert CSP Name> <Insert CSP Abbreviation, as appropriate>
CSO Name:	<Insert CSO Name> <Insert CSO Abbreviation, as appropriate>
FedRAMP Package ID:	<Insert FedRAMP Package ID>
Service Model:	<Choose one: IaaS, PaaS, SaaS, IaaS/PaaS, IaaS/PaaS/SaaS, IaaS/SaaS, PaaS/SaaS, LI-SaaS>
Digital Identity Level (DIL) Determination (SSP Appendix E):	<Choose one: IAL3/FAL3/AAL3, IAL2/FAL2/AAL2, IAL1/FAL1/AAL1>
FIPS PUB 199 Level (SSP Appendix K):	<Choose one: High, Moderate, Low, LI-SaaS>
Fully Operational as of:	<Insert MM/DD/YYYY>
Deployment Model:	<Choose one: Public Cloud, Government-Only Cloud, Hybrid Cloud>
Authorization Path:	<Choose one: Joint Authorization Board Provisional Authorization, Agency Authorization>
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.)].

Agenda

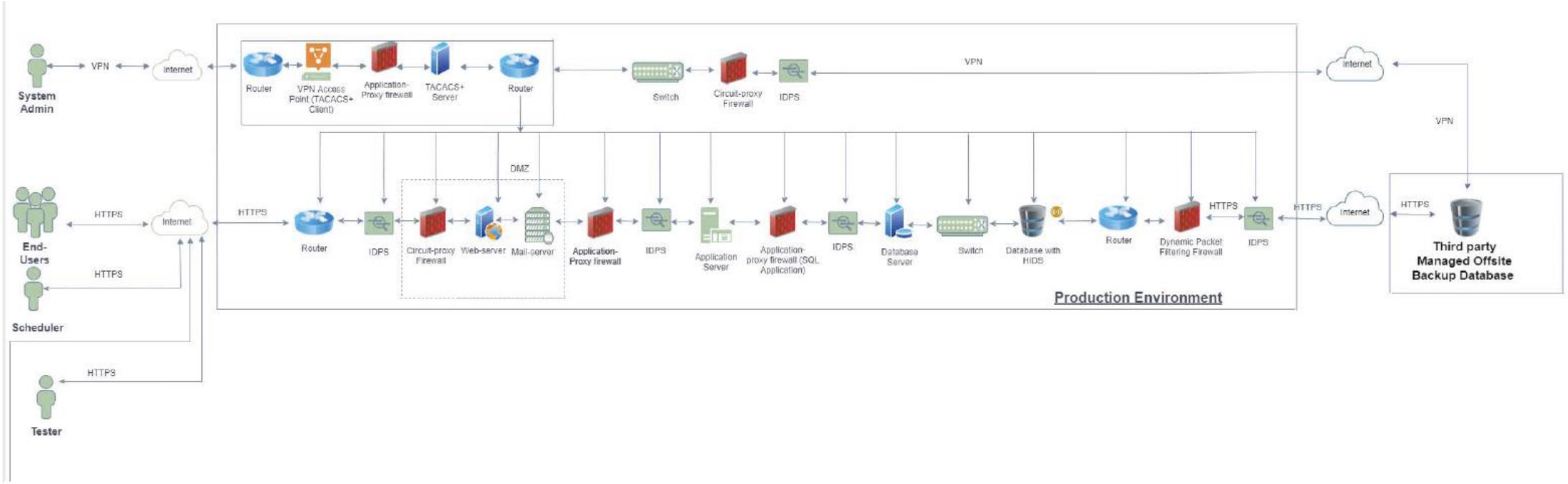
- ✓NIST Risk Management Framework – A quick review…
- ✓Implementing controls – Host hardening…
  - ✓Security configuration checklist (w/DISA STIG Viewer)
- ✓NIST 800-53Ar4 – How Controls are Assessed
- ✓SCAP - Security Content Automation Protocol
- ✓FedRAMP System Security Plan’s Section 13 – A controls 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	Due
8	1st Rough Draft System Security Plan (SSP) review	3/13
10	2nd Draft SSP review	3/27
11	3rd 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?



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…