

Defense Security Service
Industrial Security Field Operations
NISP Authorization Office (NAO)



**Technical Assessment Guide for
Windows 10 Operating System**

July 2016

Revision
Log

Date	Revision	Description of Change
2016FEB24	1.0	Initial Draft
2016JUN08	1.1	Updated formatting, Changed ODAA to NAO, Updated Baselines and Vulnerability ID's
2016JUL06	1.2	Updated language to address remote scanning, updated tool versions, added Java requirement.

Table of Contents

1.0	Tools and Documentation	4
1.1	Tools.....	4
1.1.1	SCAP Compliance Checker	4
1.1.2	DISA STIG Viewer	6
1.2	Documentation	6
2.0	Assessment Procedures.....	6
Appendix A – Control/Vulnerability ID Assessment Matrix		9

1.0 Tools and Documentation

Assessment of the technical security controls and system configuration of contractor Information Systems (IS) utilizing the Defense Information System Agency (DISA) vulnerability scanning protocols in accordance with the NISP will require the following tools and documentation:

1.1 Tools

Install these tools on the system to be scanned, or on a dedicated system for centralized (network) scanning.

1.1.1 SCAP Compliance Checker

- A. The ISSP/SCA will verify the following parameters:
- 1) Verify that the SCAP Compliance Checker is properly installed on the system that will conduct the vulnerability scan.
 - 2) Ensure that the latest version of the SCAP Compliance Checker is used. *Consult DISA's IASE website to validate the version of the SCAP Compliance Checker.*
 - 3) Ensure that the individual conducting the scans has administrator credentials for the host machine, as well as any client machines scanned across the network (if applicable). *For the purposes of network scanning, either domain-level administrator credentials or a local administrator account on the remote system is acceptable.*
 - 4) If conducting a remote scan, a system administrator will need to enable the ability to access the registry remotely on the remote system. This can be accomplished in the following manner:
 - The registry key that restricts remote access to the registry is *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg*
 - If the key to restrict access to the registry is already present in the registry, start Registry Editor and then:
 - Locate the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
 - Right-click **winreg**, click **Permissions**, and then edit the current permissions or add the users or groups to whom you want to grant access.
 - Quit Registry Editor, and then restart Windows.
 - If the key to restrict access to the registry is not present in the registry, the key will need to be created in the following manner:

- Start the registry Editor (**Regedit32.exe**) and locate the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control
 - On the **Edit** menu, click **Add Key**, and then enter the following values:
 - **Key Name:** *SecurePipeServers*
 - **Class:** *REG_SZ*
 - Locate the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers
 - On the **Edit** menu, click **Add Key**, and then enter the following values:
 - **Key Name:** *winreg*
 - **Class:** *REG_SZ*
 - Locate the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
 - On the **Edit** menu, click **Add Value**, and then enter the following values:
 - **Value Name:** *Description*
 - **Data Type:** *REG_SZ*
 - **String:** *Registry Server*
 - Locate the following key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
 - Right-click **winreg**, click **Permissions**, and then edit the current permissions or add the users or groups to whom you want to grant access.
 - Quit Registry Editor, and then restart Windows.
- 5) Verify that the ISSM/ISSO has selected the most recent appropriate Operating System benchmark within the **Edit → Content and Options** menu (e.g. *U_Windows_10_VIRI_STIG_SCAP_1-1_Benchmark*).
- The ISSP/SCA should verify on DISA’s IASE website that the most recent benchmark is loaded.
 - If the most recent benchmark is not loaded into the SCAP Compliance Checker, instruct the ISSM/ISSO to manually download and import the most recent DISA benchmark.
 - Select only one benchmark (the most recent) for the scan operation.
- 6) Verify that the ISSM/ISSO has set the SCAP Content Profile within the **Edit → Content and Options** menu for the selected benchmark to “**MAC-3 Classified**”.
- B. The ISSP/SCA will then instruct the ISSM/ISSO to execute the vulnerability scan of the system.
- C. Upon completion of the scan, the ISSP/SCA will instruct the ISSM/ISSO to retrieve the XCCDF Scan Results XML file, for import into the STIG Viewer. Unless the user has changed the repository directory manually, the XCCDF Scan Results file can be located

by navigating to **Results** → **Open Results Directory** in the SCAP tool menu, and going to the **SCAP** → **Machine Name** → **Baseline Title** → **1** → **Scan_Date** → **XML** folder.

1.1.2 DISA STIG Viewer

- A. The ISSP/SCA will do the following:
 - 1) Confirm that Java RTE is installed on the machine to be used with the STIG Viewer.
 - 2) Confirm that the DISA STIG Viewer (Version 2.3) is downloaded to a known directory.
 - 3) Confirm that the ISSM/ISSO has downloaded the most recent Operating System baseline from the DISA IASE website.
- B. Have the ISSM/ISSO import the recent baseline into the STIG Viewer, and create a checklist from the STIG baseline that includes all STIG vulnerabilities included within the baseline.

1.2 Documentation

Assessment of the technical system security controls and security configuration requires that the ISSP/SCA make risk-based decisions regarding compliance condition based on the approved/submitted plan. To facilitate the assessment the following documents will be reviewed by the ISSP/SCA:

- A. Master System Security Plan (MSSP) and/or System Security Plan (SSP)
- B. Authorization Letter (if performing a SVA)
- C. Information System Profile (IS Profile)
- D. Hardware and Software Baselines
- E. Authorized Users List and Signed User Briefings
- F. Trusted Download Procedures, Briefings and Logs
- G. Risk Acceptance Letters (if applicable)
- H. System Diagram and/or Network Topology (if applicable)
- I. DD Form 254
- J. DSS Form 147
- K. MOU/ISA's (if applicable)
- L. Manual Audit Log
- M. Removable Media Creation Log
- N. Maintenance Logs
- O. Sanitization Procedures (if applicable)
- P. Audit Variance/Hibernation Procedures (if applicable)

2.0 Assessment Procedures

In order to determine the compliance condition of the system, the ISSP/SCA along with the ISSM/ISSO will conduct the following steps:

- 1) Instruct the ISSM/ISSO to:
 - a. Navigate to the “Checklist” tab within the STIG Viewer window.
 - b. Navigate to the top menu of the STIG Viewer and click **Import → XCCDF Scan Results**.
 - c. Navigate to the directory containing the SCAP Compliance Checker XML file (filename example: *WIN-DLV2CD8RIII_SCC-4.0.1_2016-02-24_102344_XCCDF-Results_U_Windows_7_VIR27_STIG*)
 - d. Import the scan results.
 - e. In the “Target Data” drop down, select the appropriate computing role (e.g. Workstation).
 - f. In the “Technology Area” drop down, select “Windows OS”.

- 2) The ISSP/SCA will then conduct the assessment to determine satisfactory implementation of the baseline technical standards:
 - a. The ISSP/SCA may use the “CAT I/CATII/CATIII” tabs under the “Totals” dropdown to sort the vulnerabilities if desired. CAT severity values may be used to effectively prioritize assessment of vulnerabilities, but should not be cited in the vulnerability report. Ensure that vulnerability citations are mapped to their associated RMF control.
 - b. Sort the vulnerabilities by Vulnerability ID to allow for the efficient identification of the RMF control addressed by the selected Vulnerability ID (optional).
 - c. Reference the **Control/Vulnerability ID Assessment Matrix** in **Appendix A** to determine the RMF control that is applicable to the open vulnerability. This RMF control information is also contained within the “CCI” tab of each vulnerability for ease of access.
 - d. Consult the System Security Plan and any associated or supporting documentation to determine if the control is satisfactorily implemented, mitigated, tailored out, or non-compliant (open).
 - e. Record any open vulnerabilities, follow-up or mitigation actions, and POAM’s (if applicable) in the Vulnerability Assessment Report.

**** THIS PAGE INTENTIONALLY LEFT BLANK ****

Appendix A – Control/Vulnerability ID Assessment Matrix

The below matrix can be used to reconcile RMF controls with SCAP/STIG Vulnerability ID's.

Legend:

- **Control ID:** NIST 800-53 Rev 4 RMF Control Identifier
- **Vuln. ID:** STIG Vulnerability Identifier
- **O:** OPEN Vulnerability (Non-Compliant)
- **M:** OPEN Vulnerability, Mitigated by facility (Compliant). Document mitigation in Vulnerability Report.
- **C:** CLOSED Vulnerability (Compliant)
- **N/A:** Tailored Out in Plan, or Not Applicable to System Type (Compliant)
- **Description:** Short description of system setting and/or control requirements.

Control ID	Vuln ID	O	M	C	N/A	Description	Notes
AC-2 (4)	V-63443					The system must be configured to audit Account Management - Security Group Management failures.	
	V-63445					The system must be configured to audit Account Management - Security Group Management successes.	
	V-63447					The system must be configured to audit Account Management - User Account Management failures.	
	V-63449					The system must be configured to audit Account Management - User Account Management successes.	
AC-3	V-63353					Local volumes must be formatted using NTFS.	
	V-63845					The Access this computer from the network user right must only be assigned to the Administrators group.	
	V-63851					The Allow log on locally user right must only be assigned to the Administrators and Users groups.	
	V-63871					The Deny access to this computer from the network user right on workstations must be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and	

					unauthenticated access on all systems.	
	V-63873				The Deny log on as a batch job user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.	
	V-63875				The Deny log on as a service user right on domain-joined workstations must be configured to prevent access from highly privileged domain accounts.	
	V-63877				The Deny log on locally user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems and unauthenticated access on all systems.	
	V-63879				The Deny log on through Remote Desktop Services user right on workstations must at a minimum be configured to prevent access from highly privileged domain accounts and local accounts on domain systems and unauthenticated access on all systems.	
AC-3 (4)	V-63373				Permissions for system files and directories must conform to minimum requirements.	
AC-6 (10)	V-63361				Only accounts responsible for the administration of a system must have Administrator rights on the system.	
	V-63593				Default permissions for the HKEY_LOCAL_MACHINE registry hive must be maintained.	
	V-63843				The Access Credential Manager as a trusted caller user right must not be assigned to any groups or accounts.	
	V-63847				The Act as part of the operating system user right must not be assigned to any groups or accounts.	
	V-63849				The Adjust memory quotas for a process user right must only be assigned to Administrators Local Service and Network Service.	

V-63853					The Back up files and directories user right must only be assigned to the Administrators group.	
V-63855					The Change the system time user right must only be assigned to Administrators and Local Service.	
V-63857					The Create a pagefile user right must only be assigned to the Administrators group.	
V-63859					The Create a token object user right must not be assigned to any groups or accounts.	
V-63861					The Create global objects user right must only be assigned to Administrators Service Local Service and Network Service.	
V-63863					The Create permanent shared objects user right must not be assigned to any groups or accounts.	
V-63865					The Create symbolic links user right must only be assigned to the Administrators group.	
V-63869					The Debug programs user right must only be assigned to the Administrators group.	
V-63881					The Enable computer and user accounts to be trusted for delegation user right must not be assigned to any groups or accounts.	
V-63883					The Force shutdown from a remote system user right must only be assigned to the Administrators group.	
V-63887					The Generate security audits user right must only be assigned to Local Service and Network Service.	
V-63889					The Impersonate a client after authentication user right must only be assigned to Administrators Service Local Service and Network Service.	
V-63891					The Increase scheduling priority user right must only be assigned to the Administrators group.	
V-63917					The Load and unload device drivers user right must only be assigned to the Administrators group.	
V-63925					The Lock pages in memory user right must not be assigned to any groups or accounts.	

	V-63929					The Modify an object label user right must not be assigned to any groups or accounts.	
	V-63931					The Modify firmware environment values user right must only be assigned to the Administrators group.	
	V-63933					The Perform volume maintenance tasks user right must only be assigned to the Administrators group.	
	V-63935					The Profile single process user right must only be assigned to the Administrators group.	
	V-63937					The Replace a process level token user right must only be assigned to Local Service and Network Service.	
	V-63939					The Restore files and directories user right must only be assigned to the Administrators group.	
	V-63941					The Take ownership of files or other objects user right must only be assigned to the Administrators group.	
AC-7 a	V-63409					The number of allowed bad logon attempts must be configured to 3 or less.	
	V-63413					The period of time before the bad logon counter is reset must be configured to 15 minutes.	
AC-7 b	V-63405					The lockout duration must be configured to require an administrator to unlock an account.	
AC-8 a	V-63675					The required legal notice must be configured to display before console logon.	
	V-63681					The Windows dialog box title for the legal banner must be configured.	
AC-11 (1)	V-63835					A screen saver must be enabled on the system.	
AC-11 a	V-63669					The machine inactivity limit must be set to 15 minutes locking the system with the screensaver.	
AC-11 b	V-63837					The screen saver must be password protected.	
AC-17 (1)	V-63459					The system must be configured to audit Logon/Logoff - Logoff successes.	
	V-63463					The system must be configured to audit Logon/Logoff - Logon failures.	

	V-63467					The system must be configured to audit Logon/Logoff - Logon successes.	
AC-17 (2)	V-63737					The Remote Desktop Session Host must require secure RPC communications.	
	V-63741					Remote Desktop Services must be configured with the client connection encryption set to the required level.	
AU-12 c	V-63431					The system must be configured to audit Account Logon - Credential Validation failures.	
	V-63435					The system must be configured to audit Account Logon - Credential Validation successes.	
	V-63439					The system must be configured to audit Account Management - Other Account Management Events failures.	
	V-63441					The system must be configured to audit Account Management - Other Account Management Events successes.	
	V-63451					The system must be configured to audit Detailed Tracking - PNP Activity successes.	
	V-63453					The system must be configured to audit Detailed Tracking - Process Creation successes.	
	V-63455					The system must be configured to audit Logon/Logoff - Account Lockout successes.	
	V-63457					The system must be configured to audit Logon/Logoff - Group Membership successes.	
	V-63469					The system must be configured to audit Logon/Logoff - Special Logon successes.	
	V-63471					The system must be configured to audit Object Access - Removable Storage failures.	
	V-63473					The system must be configured to audit Object Access - Removable Storage successes.	
V-63475					The system must be configured to audit Policy Change - Audit Policy Change failures.		

	V-63479	Red	Yellow	Green		The system must be configured to audit Policy Change - Audit Policy Change successes.	
	V-63481	Red	Yellow	Green		The system must be configured to audit Policy Change - Authentication Policy Change successes.	
	V-63483	Red	Yellow	Green		The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
	V-63487	Red	Yellow	Green		The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
	V-63491	Red	Yellow	Green		The system must be configured to audit System - IPsec Driver failures.	
	V-63495	Red	Yellow	Green		The system must be configured to audit System - IPsec Driver successes.	
	V-63499	Red	Yellow	Green		The system must be configured to audit System - Other System Events successes.	
	V-63503	Red	Yellow	Green		The system must be configured to audit System - Other System Events failures.	
	V-63507	Red	Yellow	Green		The system must be configured to audit System - Security State Change successes.	
	V-63511	Red	Yellow	Green		The system must be configured to audit System - Security System Extension failures.	
	V-63513	Red	Yellow	Green		The system must be configured to audit System - Security System Extension successes.	
	V-63515	Red	Yellow	Green		The system must be configured to audit System - System Integrity failures.	
	V-63517	Red	Yellow	Green		The system must be configured to audit System - System Integrity successes.	
	V-63635	Red	Yellow	Green		Audit policy using subcategories must be enabled.	
AU-4	V-63519	Red	Yellow	Green		The Application event log size must be configured to 32768 KB or greater.	
	V-63523	Red	Yellow	Green		The Security event log size must be configured to 196608 KB or greater.	
	V-63527	Red	Yellow	Green		The System event log size must be configured to 32768 KB or greater.	

AU-9	V-63533	Red	Yellow	Green	Grey	Permissions for the Application event log must prevent access by non-privileged accounts.	
	V-63537	Red	Yellow	Green	Grey	Permissions for the Security event log must prevent access by non-privileged accounts.	
	V-63541	Red	Yellow	Green	Grey	Permissions for the System event log must prevent access by non-privileged accounts.	
	V-63927	Red	Yellow	Green	Grey	The Manage auditing and security log user right must only be assigned to the Administrators group.	
CM-11 (2)	V-63321	Red	Yellow	Green	Grey	Users must be prevented from changing installation options.	
	V-63325	Red	Yellow	Green	Grey	The Windows Installer Always install with elevated privileges must be disabled.	
CM-6 b	V-63319	Red	Yellow	Green	Grey	Domain-joined systems must use Windows 10 Enterprise Edition.	
	V-63323	Red	Yellow	Green	Grey	Domain-joined systems must have a Trusted Platform Module (TPM) enabled and ready for use.	
	V-63327	Red	Yellow	Green	Grey	System firmware or system controllers must have administrator accounts/passwords configured.	
	V-63329	Red	Yellow	Green	Grey	Users must be notified if a web-based program attempts to install software.	
	V-63331	Red	Yellow	Green	Grey	The system must not use removable media as the boot loader.	
	V-63333	Red	Yellow	Green	Grey	Automatically signing in the last interactive user after a system-initiated restart must be disabled.	
	V-63349	Red	Yellow	Green	Grey	Systems must be maintained at a supported servicing level.	
	V-63351	Red	Yellow	Green	Grey	An approved up-to-date DoD antivirus program must be installed and used.	
	V-63355	Red	Yellow	Green	Grey	Alternate operating systems must not be permitted on the same system.	
	V-63363	Red	Yellow	Green	Grey	Only accounts responsible for the backup operations must be members of the Backup Operators group.	
	V-63367	Red	Yellow	Green	Grey	Standard local user accounts must not exist on a system in a domain.	

V-63379					The Enhanced Mitigation Experience Toolkit (EMET) v5.5 or later must be installed on the system.	
V-63393					Software certificate installation files must be removed from a system.	
V-63395					The HBSS McAfee Agent must be installed.	
V-63399					A host-based firewall must be installed and enabled on the system.	
V-63403					Inbound exceptions to the firewall on domain workstations must only allow authorized remote management hosts.	
V-63529					The system must be configured to send error reports on TCP port 1232.	
V-63551					Automatic logons must be disabled.	
V-63555					IPv6 source routing must be configured to highest protection.	
V-63559					The system must be configured to prevent IP source routing.	
V-63563					The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	
V-63569					Insecure logons to an SMB server must be disabled.	
V-63573					All Direct Access traffic must be routed through the internal network.	
V-63577					Hardened UNC Paths must be defined to require mutual authentication and integrity for at least the *\SYSVOL and *\NETLOGON shares.	
V-63581					Simultaneous connections to the Internet or a Windows domain must be limited.	
V-63585					Connections to non-domain networks when connected to a domain authenticated network must be blocked.	
V-63591					Wi-Fi Sense must be disabled.	

V-63595					Virtualization Based Security must be enabled with the platform security level configured to Secure Boot with DMA Protection.	
V-63599					Credential Guard must be running on domain-joined systems.	
V-63603					Virtualization-based protection of code integrity must be enabled on domain-joined systems.	
V-63607					Early Launch Antimalware Boot-Start Driver Initialization Policy must prevent boot drivers identified as bad.	
V-63609					Group Policy objects must be reprocessed even if they have not changed.	
V-63613					Group Policies must be refreshed in the background if the user is logged on.	
V-63617					Local accounts with blank passwords must be restricted to prevent access from the network.	
V-63619					The built-in administrator account must be renamed.	
V-63625					The built-in guest account must be renamed.	
V-63627					Systems must at least attempt device authentication using certificates.	
V-63641					The system must be configured to block untrusted fonts from loading.	
V-63653					The computer account password must not be prevented from being reset.	
V-63659					The setting to allow Microsoft accounts to be optional for modern style apps must be enabled.	
V-63661					The maximum age for machine account passwords must be configured to 30 days or less.	
V-63677					Enhanced anti-spoofing when available must be enabled for facial recognition.	
V-63683					Windows Telemetry must be configured to the lowest level of data sent to Microsoft.	
V-63687					Caching of logon credentials must be limited.	

V-63693					Domain Controller authentication must not be required to unlock the workstation.	
V-63695					File Explorer shell protocol must run in protected mode.	
V-63697					The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	
V-63699					Users must not be allowed to ignore SmartScreen filter warnings for malicious websites in Microsoft Edge.	
V-63701					Users must not be allowed to ignore SmartScreen filter warnings for unverified files in Microsoft Edge.	
V-63705					InPrivate browsing in Microsoft Edge must be disabled.	
V-63709					The password manager function in the Edge browser must be disabled.	
V-63713					The SmartScreen filter for Microsoft Edge must be enabled.	
V-63717					The use of a hardware security device with Microsoft Passport for Work must be enabled.	
V-63721					The minimum pin length for Microsoft Passport for Work must be 6 characters or greater.	
V-63735					The service principal name (SPN) target name validation level must be configured to Accept if provided by client.	
V-63739					Anonymous SID/Name translation must not be allowed.	
V-63743					Attachments must be prevented from being downloaded from RSS feeds.	
V-63745					Anonymous enumeration of SAM accounts must not be allowed.	
V-63755					The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	
V-63765					NTLM must be prevented from falling back to a Null session.	

	V-63767	Red	Yellow	Green	Grey	PKU2U authentication using online identities must be prevented.	
	V-63801	Red	Yellow	Green	Grey	The LanMan authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	
	V-63803	Red	Yellow	Green	Grey	The system must be configured to the required LDAP client signing level.	
	V-63805	Red	Yellow	Green	Grey	The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.	
	V-63807	Red	Yellow	Green	Grey	The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.	
	V-63809	Red	Yellow	Green	Grey	The Recovery Console option must be set to prevent automatic logon to the system.	
	V-63813	Red	Yellow	Green	Grey	The system must be configured to require case insensitivity for non-Windows subsystems.	
	V-63815	Red	Yellow	Green	Grey	The default permissions of global system objects must be increased.	
	V-63841	Red	Yellow	Green	Grey	Zone information must be preserved when saving attachments.	
	V-63957	Red	Yellow	Green	Grey	The machine account lockout threshold must be set to 10 on systems with BitLocker enabled.	
	V-65681	Red	Yellow	Green	Grey	Windows Update must not obtain updates from other PCs on the Internet.	
CM-7 (2)	V-63667	Red	Yellow	Green	Grey	Autoplay must be turned off for non-volume devices.	
	V-63671	Red	Yellow	Green	Grey	The default autorun behavior must be configured to prevent autorun commands.	
	V-63673	Red	Yellow	Green	Grey	Autoplay must be disabled for all drives.	
CM-7 (5) (b)	V-63345	Red	Yellow	Green	Grey	The operating system must employ a deny-all permit-by-exception policy to allow the execution of authorized software programs.	
CM-7 a	V-63365	Red	Yellow	Green	Grey	Users must not be allowed to run virtual machines in Hyper-V on the system.	

	V-63377					Internet Information System (IIS) or its subcomponents must not be installed on a workstation.	
	V-63383					Simple TCP/IP Services must not be installed on the system.	
	V-63747					Basic authentication for RSS feeds over HTTP must not be used.	
	V-63751					Indexing of encrypted files must be turned off.	
	V-63545					Camera access from the lock screen must be disabled.	
	V-63549					The display of slide shows on the lock screen must be disabled.	
	V-63615					Downloading print driver packages over HTTP must be prevented.	
	V-63621					Web publishing and online ordering wizards must be prevented from downloading a list of providers.	
	V-63623					Printing over HTTP must be prevented.	
	V-63629					The network selection user interface (UI) must not be displayed on the logon screen.	
	V-63631					Connected users on domain-joined computers must not be enumerated.	
	V-63633					Local users on domain-joined computers must not be enumerated.	
	V-63637					Signing in using a PIN must be turned off.	
	V-63663					The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	
	V-63685					The Windows SmartScreen must be configured to require approval from an administrator before running downloaded unknown software.	
	V-63725					The use of OneDrive for storage must be disabled.	
	V-63839					Toast notifications to the lock screen must be turned off.	
CM-7 b	V-63381					Simple Network Management Protocol (SNMP) must not be installed on the system.	

	V-63385					The Telnet Client must not be installed on the system.	
	V-63389					The TFTP Client must not be installed on the system.	
IA-11	V-63375					The Windows Remote Management (WinRM) service must not store RunAs credentials.	
	V-63753					The system must be configured to prevent the storage of passwords and credentials.	
	V-63645					Users must be prompted for a password on resume from sleep (on battery).	
	V-63649					The user must be prompted for a password on resume from sleep (plugged in).	
	V-63729					Passwords must not be saved in the Remote Desktop Client.	
	V-63733					Remote Desktop Services must always prompt a client for passwords upon connection.	
	V-63817					User Account Control approval mode for the built-in Administrator must be enabled.	
	V-63821					User Account Control must automatically deny elevation requests for standard users.	
	V-63829					User Account Control must run all administrators in Admin Approval Mode enabling UAC.	
	IA-2	V-63601				The built-in administrator account must be disabled.	
IA-3	V-63763				Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.		
IA-3 (1)	V-63655					Client computers must be required to authenticate for RPC communication.	
	V-63657					Unauthenticated RPC clients must be restricted from connecting to the RPC server.	
IA-4 e	V-63359					Unused accounts must be disabled or removed from the system after 35 days of inactivity.	
IA-5 (1) (a)	V-63423					Passwords must at a minimum be 14 characters.	
	V-63427					The built-in Microsoft password complexity filter	

						must be enabled.	
IA-5 (1) (d)	V-63371					Accounts must be configured to require password expiration.	
	V-63419					The maximum password age must be configured to 60 days or less.	
	V-63421					The minimum password age must be configured to at least 1 day.	
IA-5 (1) c	V-63429					Reversible password encryption must be disabled.	
	V-63797					The system must be configured to prevent the storage of the LAN Manager hash of passwords.	
	V-63711					Unencrypted passwords must not be sent to third-party SMB Servers.	
IA-5 (1) e	V-63415					The password history must be configured to 24 passwords remembered.	
IA-5 (2) (a)	V-63579					The DoD Root Certificate must be installed into the Trusted Root Store.	
	V-63583					The External CA Root Certificate must be installed into the Trusted Root Store.	
	V-63587					The DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate must be installed into the Untrusted Certificates Store.	
	V-63589					The US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate must be installed into the Untrusted Certificates Store.	
IA-7	V-63795					Kerberos encryption types must be configured to prevent the use of DES and RC4 encryption suites.	
IA-8	V-63611					The built-in guest account must be disabled.	
MA-4 (6)	V-63339					The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	
	V-63369					The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	
MA-4 c	V-63335					The Windows Remote Management (WinRM) client must not use Basic authentication.	

	V-63341					The Windows Remote Management (WinRM) client must not use Digest authentication.	
	V-63347					The Windows Remote Management (WinRM) service must not use Basic authentication.	
SC-10	V-63715					The amount of idle time required before suspending a session must be configured to 15 minutes or less.	
	V-63727					Users must be forcibly disconnected when their logon hours expire.	
	V-63799					The system must be configured to force users to log off when their allowed logon hours expire.	
SC-13	V-63811					The system must be configured to use FIPS-compliant algorithms for encryption hashing and signing.	
SC-28	V-63337					Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.	
SC-3	V-63597					Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	
	V-63679					Administrator accounts must not be enumerated during elevation.	
	V-63819					User Account Control must at minimum prompt administrators for consent on the secure desktop.	
	V-63825					User Account Control must be configured to detect application installations and prompt for elevation.	
	V-63827					User Account Control must only elevate UIAccess applications that are installed in secure locations.	
	V-63831					User Account Control must virtualize file and registry write failures to per-user locations.	
SC-4	V-63651					Solicited Remote Assistance must not be allowed.	
	V-63731					Local drives must be prevented from sharing with Remote Desktop Session Hosts.	

	V-63357					Non system-created file shares on a system must limit access to groups that require it.	
	V-63749					Anonymous enumeration of shares must be restricted.	
	V-63759					Anonymous access to Named Pipes and Shares must be restricted.	
	V-63761					The system must be configured to use the Classic security model.	
SC-5	V-63567					The system must be configured to ignore NetBIOS name release requests except from WINS servers.	
	V-63691					Turning off File Explorer heap termination on corruption must be disabled.	
SC-8	V-63525					The system must be configured to use SSL to forward error reports.	
	V-63643					Outgoing secure channel traffic must be encrypted when possible.	
	V-63647					Outgoing secure channel traffic must be signed when possible.	
	V-63665					The system must be configured to require a strong session key.	
	V-63703					The Windows SMB client must be configured to always perform SMB packet signing.	
	V-63707					The Windows SMB client must be enabled to perform SMB packet signing when possible.	
	V-63719					The Windows SMB server must be configured to always perform SMB packet signing.	
	V-63723					The Windows SMB server must perform SMB packet signing when possible.	
SC-8 (1)	V-63639				Outgoing secure channel traffic must be encrypted or signed.		
SI-11 a	V-63461					The system must be configured to generate error reports.	
	V-63489					The system must be configured to save Error Reporting events and messages to the system event log.	

	V-63521	Red	Yellow	Green	Grey	The system must be configured to store error reports locally on the system or in the enclave and not send them to Microsoft.	
	V-63535	Red	Yellow	Green	Grey	The system must be configured to archive error reports.	
	V-63539	Red	Yellow	Green	Grey	The system must be configured to store all data in the error report archive.	
	V-63543	Red	Yellow	Green	Grey	The maximum number of error reports to archive on a system must be configured to 100 or greater.	
	V-63547	Red	Yellow	Green	Grey	The system must be configured to queue error reports until a local or DOD-wide collector is available.	
	V-63557	Red	Yellow	Green	Grey	The system must be configured to add all error reports to the queue.	
	V-63561	Red	Yellow	Green	Grey	The maximum number of error reports to queue on a system must be configured to 50 or greater.	
	V-63565	Red	Yellow	Green	Grey	The system must be configured to attempt to forward queued error reports once a day.	
	V-63571	Red	Yellow	Green	Grey	The system must be configured to automatically consent to send all data requested by a local or DOD-wide error collection site.	
	V-63575	Red	Yellow	Green	Grey	The system must be configured to permit the default consent levels of Windows Error Reporting to override any other consent policy setting.	
	V-63437	Red	Yellow	Green	Grey	The Windows Error Reporting Service must be running and configured to start automatically.	
SI-11 b	V-63493	Red	Yellow	Green	Grey	The system must be configured to allow a local or DOD-wide collector to request additional error reporting diagnostic data to be sent.	
	V-63497	Red	Yellow	Green	Grey	The system must be configured to collect multiple error reports of the same event type.	
	V-63505	Red	Yellow	Green	Grey	The system must be configured to prevent the display of error messages to the user.	
SI-16	V-63387	Red	Yellow	Green	Grey	The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer	

					must be enabled.	
	V-63391				The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software must be enabled.	
	V-63401				The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomization (ASLR) must be enabled and configured to Application Opt In.	
	V-63407				The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) must be enabled and configured to at least Application Opt Out.	
	V-63411				The Enhanced Mitigation Experience Toolkit (EMET) system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be configured to Application Opt Out.	
	V-63417				The Enhanced Mitigation Experience Toolkit (EMET) Default Actions and Mitigations Settings must enable Deep Hooks.	
	V-63425				The Enhanced Mitigation Experience Toolkit (EMET) Default Actions and Mitigations Settings must enable Anti Detours.	
	V-63433				The Enhanced Mitigation Experience Toolkit (EMET) Default Actions and Mitigations Settings must enable Banned Functions.	
	V-63689				Explorer Data Execution Prevention must be enabled.	
	V-63397				The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Recommended Software must be enabled.	
SI-2 (2)	V-63343				The operating system must employ automated mechanisms to determine the state of system components with regard to flaw remediation using the following frequency: continuously where HBSS is used; 30 days for any additional internal network	

						scans not covered by HBSS; and annually for external scans by Computer Network Defense Service Provider (CNDSP).	
--	--	--	--	--	--	--	--