

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



**Technical Assessment Guide for
Windows Server 2012 Domain
Controller**

July 2016

Revision
Log

Date	Revision	Description of Change
2016FEB24	1.0	Initial Draft
2016JUN14	1.1	Updated formatting, Changed ODAA to NAO, Updated Baselines and Vulnerability ID's
2016JUL06	1.2	Updated content 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	5
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	Rule Title	Notes
AC-10	V-3449					Remote Desktop Services must limit users to one remote session.	
AC-11 (1)	V-36656					A screen saver must be enabled on the system.	
	V-36774					A screen saver must be defined.	
	V-36775					Changing the screen saver must be prevented.	
AC-11 a	V-36773				The machine inactivity limit must be set to 15 minutes locking the system with the screensaver.		
AC-11 b	V-36657				The screen saver must be password protected.		
AC-17 (1)	V-26540					The system must be configured to audit Logon/Logoff - Logoff successes.	
	V-26542					The system must be configured to audit Logon/Logoff - Logon failures.	
	V-26541					The system must be configured to audit Logon/Logoff - Logon successes.	
	V-15997					Users must be prevented from mapping local COM ports and redirecting data from the Remote Desktop Session Host to local COM ports. (Remote Desktop Services Role).	

	V-15998					Users must be prevented from mapping local LPT ports and redirecting data from the Remote Desktop Session Host to local LPT ports. (Remote Desktop Services Role).	
	V-15999					Users must be prevented from redirecting Plug and Play devices to the Remote Desktop Session Host. (Remote Desktop Services Role).	
	V-16005					The system must be configured to remove the Disconnect option from the Shut Down dialog box on the Remote Desktop Client. (Remote Desktop Services Role).	
	V-16000					The system must be configured to ensure smart card devices can be redirected to the Remote Desktop session. (Remote Desktop Services Role).	
AC-17 (2)	V-3454					Remote Desktop Services must be configured with the client connection encryption set to the required level.	
	V-4447					The Remote Desktop Session Host must require secure RPC communications.	
AC-2 (2)	V-57653					The operating system must automatically remove or disable temporary user accounts after 72 hours.	
	V-57655					The operating system must be configured such that emergency administrator accounts are never automatically removed or disabled.	
AC-2 (4)	V-26536					The system must be configured to audit Account Management - Security Group Management failures.	
	V-26535					The system must be configured to audit Account Management - Security Group Management successes.	
	V-26538					The system must be configured to audit Account Management - User Account Management failures.	
	V-26537					The system must be configured to audit Account Management - User Account Management successes.	
AC-3	V-26470				Unauthorized accounts must not have the Access this computer from the network user right on domain controllers.		

	V-26472				Unauthorized accounts must not have the Allow log on locally user right.	
	V-26473				Unauthorized accounts must not have the Allow log on through Remote Desktop Services user right.	
	V-1155				The Deny access to this computer from the network user right on domain controllers must be configured to prevent unauthenticated access.	
	V-26483				The Deny log on as a batch job user right on domain controllers must be configured to prevent unauthenticated access.	
	V-26484				The Deny log on as a service user right must be configured to include no accounts or groups (blank) on domain controllers.	
	V-26485				The Deny log on locally user right on domain controllers must be configured to prevent unauthenticated access.	
	V-26486				The Deny log on through Remote Desktop Services user right on domain controllers must be configured to prevent unauthenticated access.	
	V-26495				Unauthorized accounts must not have the Log on as a batch job user right.	
	V-1081				Local volumes must be formatted using NTFS.	
	V-1135				Nonadministrative user accounts or groups must only have print permissions on printer shares.	
AC-3 (4)	V-40178				Permissions for system drive root directory (usually C:\) must conform to minimum requirements.	
	V-40177				Permissions for program file directories must conform to minimum requirements.	
AC-6 (10)	V-26469				Unauthorized accounts must not have the Access Credential Manager as a trusted caller user right.	
	V-30016				Unauthorized accounts must not have the Add workstations to domain user right.	

V-26471					Unauthorized accounts must not have the Adjust memory quotas for a process user right.	
V-1152					Anonymous access to the registry must be restricted.	
V-26474					Unauthorized accounts must not have the back up files and directories user right.	
V-26475					Unauthorized accounts must not have the Bypass traverse checking user right.	
V-26476					Unauthorized accounts must not have the Change the system time user right.	
V-26478					Unauthorized accounts must not have the Create a pagefile user right.	
V-26479					Unauthorized accounts must not have the Create a token object user right.	
V-26480					Unauthorized accounts must not have the Create global objects user right.	
V-26481					Unauthorized accounts must not have the Create permanent shared objects user right.	
V-26482					Unauthorized accounts must not have the Create symbolic links user right.	
V-8316					Active Directory data files must have proper access control permissions.	
V-26487					Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right on domain controllers.	
V-26488					Unauthorized accounts must not have the Force shutdown from a remote system user right.	
V-26489					Unauthorized accounts must not have the Generate security audits user right.	
V-33673					Active Directory Group Policy objects must have proper access control permissions.	
V-26490					Unauthorized accounts must not have the Impersonate a client after authentication user right.	

V-26491					Unauthorized accounts must not have the Increase a process working set user right.	
V-26492					Unauthorized accounts must not have the Increase scheduling priority user right.	
V-26493					Unauthorized accounts must not have the Load and unload device drivers user right.	
V-26494					Unauthorized accounts must not have the Lock pages in memory user right.	
V-26497					Unauthorized accounts must not have the Modify an object label user right.	
V-26498					Unauthorized accounts must not have the Modify firmware environment values user right.	
V-26499					Unauthorized accounts must not have the Perform volume maintenance tasks user right.	
V-26500					Unauthorized accounts must not have the Profile single process user right.	
V-26501					Unauthorized accounts must not have the Profile system performance user right.	
V-26503					Unauthorized accounts must not have the Replace a process level token user right.	
V-26504					Unauthorized accounts must not have the Restore files and directories user right.	
V-1127					Only administrators responsible for the domain controller must have Administrator rights on the system.	
V-26505					Unauthorized accounts must not have the Shut down the system user right.	
V-12780					The Synchronize directory service data user right must be configured to include no accounts or groups (blank).	
V-26506					Unauthorized accounts must not have the Take ownership of files or other objects user right.	
V-1102					Unauthorized accounts must not have the Act as part of the operating system user right.	

	V-18010					Unauthorized accounts must not have the Debug programs user right.	
	V-39331					The Active Directory SYSVOL directory must have the proper access control permissions.	
	V-39332					The Active Directory Domain Controllers Organizational Unit (OU) object must have the proper access control permissions.	
	V-39333					Domain created Active Directory Organizational Unit (OU) objects must have proper access control permissions.	
	V-26070					Standard user accounts must only have Read permissions to the Winlogon registry key.	
	V-32282					Standard user accounts must only have Read permissions to the Active Setup\Installed Components registry key.	
AC-7 a	V-1097					The number of allowed bad logon attempts must meet minimum requirements.	
	V-1098					The period of time before the bad logon counter is reset must meet minimum requirements.	
AC-7 b	V-1099					The lockout duration must be configured to require an administrator to unlock an account.	
AC-8 a	V-26359					The Windows dialog box title for the legal banner must be configured.	
	V-1089					The required legal notice must be configured to display before console logon.	
AU-10	V-36722					Permissions for the Application event log must prevent access by nonprivileged accounts.	
AU-11	V-36723					Permissions for the Security event log must prevent access by nonprivileged accounts.	
AU-12	V-36724					Permissions for the System event log must prevent access by nonprivileged accounts.	
AU-12 a	V-14230					Audit policy using subcategories must be enabled.	

AU-12 c	V-26546	Red	Yellow	Green	Grey	The system must be configured to audit Policy Change - Audit Policy Change successes.	
	V-26530	Red	Yellow	Green	Grey	The system must be configured to audit Account Logon - Credential Validation failures.	
	V-26529	Red	Yellow	Green	Grey	The system must be configured to audit Account Logon - Credential Validation successes.	
	V-26552	Red	Yellow	Green	Grey	The system must be configured to audit System - IPsec Driver failures.	
	V-26551	Red	Yellow	Green	Grey	The system must be configured to audit System - IPsec Driver successes.	
	V-26539	Red	Yellow	Green	Grey	The system must be configured to audit Detailed Tracking - Process Creation successes.	
	V-26543	Red	Yellow	Green	Grey	The system must be configured to audit Logon/Logoff - Special Logon successes.	
	V-36667	Red	Yellow	Green	Grey	The system must be configured to audit Object Access - Removable Storage failures.	
	V-36668	Red	Yellow	Green	Grey	The system must be configured to audit Object Access - Removable Storage successes.	
	V-57633	Red	Yellow	Green	Grey	The system must be configured to audit Policy Change - Authorization Policy Change successes.	
	V-57635	Red	Yellow	Green	Grey	The system must be configured to audit Policy Change - Authorization Policy Change failures.	
	V-40202	Red	Yellow	Green	Grey	The system must be configured to audit Object Access - Central Access Policy Staging successes.	
	V-40200	Red	Yellow	Green	Grey	The system must be configured to audit Object Access - Central Access Policy Staging failures.	
	V-26547	Red	Yellow	Green	Grey	The system must be configured to audit Policy Change - Audit Policy Change failures.	
	V-26548	Red	Yellow	Green	Grey	The system must be configured to audit Policy Change - Authentication Policy Change successes.	
V-26532	Red	Yellow	Green	Grey	The system must be configured to audit Account Management - Computer Account Management failures.		

V-26531					The system must be configured to audit Account Management - Computer Account Management successes.	
V-33664					The system must be configured to audit DS Access - Directory Service Access failures.	
V-33663					The system must be configured to audit DS Access - Directory Service Access successes.	
V-33666					The system must be configured to audit DS Access - Directory Service Changes failures.	
V-33665					The system must be configured to audit DS Access - Directory Service Changes successes.	
V-26534					The system must be configured to audit Account Management - Other Account Management Events failures.	
V-26533					The system must be configured to audit Account Management - Other Account Management Events successes.	
V-26554					The system must be configured to audit System - Security State Change failures.	
V-26553					The system must be configured to audit System - Security State Change successes.	
V-26556					The system must be configured to audit System - Security System Extension failures.	
V-26555					The system must be configured to audit System - Security System Extension successes.	
V-26550					The system must be configured to audit Privilege Use - Sensitive Privilege Use failures.	
V-26549					The system must be configured to audit Privilege Use - Sensitive Privilege Use successes.	
V-26558					The system must be configured to audit System - System Integrity failures.	
V-26557					The system must be configured to audit System - System Integrity successes.	

	V-39325					Active Directory Group Policy objects must be configured with proper audit settings.	
	V-39326					The Active Directory Domain object must be configured with proper audit settings.	
	V-39327					The Active Directory Infrastructure object must be configured with proper audit settings.	
	V-39328					The Active Directory Domain Controllers Organizational Unit (OU) object must be configured with proper audit settings.	
	V-39329					The Active Directory AdminSDHolder object must be configured with proper audit settings.	
	V-39330					The Active Directory RID Manager\$ object must be configured with proper audit settings.	
AU-3 (1)	V-43239					Command line data must be prevented from inclusion in process creation events (Windows 2012 R2).	
AU-4	V-26579					The Application event log size must be configured to 32768 KB or greater.	
	V-26580					The Security event log size must be configured to 196608 KB or greater.	
	V-26581					The Setup event log size must be configured to 32768 KB or greater.	
	V-26582					The System event log size must be configured to 32768 KB or greater.	
AU-4 (1)	V-36672					Audit records must be backed up onto a different system or media than the system being audited.	
	V-57719					The operating system must at a minimum off-load audit records of interconnected systems in real time and off-load standalone systems weekly.	
AU-5 (2) (a)	V-14820					Domain Controller PKI certificates must be issued by the DoD PKI or an approved External Certificate Authority (ECA).	
	V-26683					PKI certificates associated with user accounts must be issued by the DoD PKI or an approved External Certificate Authority (ECA).	

	V-32272					The DoD root certificate must be installed into the Trusted Root Store.	
	V-32274					The DoD Interoperability Root CA 1 to DoD Root CA 2 cross-certificate must be installed into the Untrusted Certificates Store.	
	V-40237					The US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate must be installed into the Untrusted Certificates Store.	
	V-39334					Domain controllers must have a PKI server certificate.	
AU-5 a	V-4108					The system must generate an audit event when the audit log reaches a percentage of full threshold.	
AU-8 (1) (a)	V-8322					Time synchronization must be enabled on the domain controller.	
	V-3472					If the time service is configured it must use an authorized time server.	
AU-9	V-26496					Unauthorized accounts must not have the Manage auditing and security log user right.	
	V-57721					Event Viewer must be protected from unauthorized modification and deletion.	
CM-11 (2)	V-34974					The Windows Installer Always install with elevated privileges option must be disabled.	
	V-15703					Users must not be prompted to search Windows Update for device drivers.	
	V-3480					Windows Media Player must be configured to prevent automatic checking for updates.	
	V-3481					Media Player must be configured to prevent automatic Codec downloads.	
	V-21965					Device driver searches using Windows Update must be prevented.	
	V-1151					The print driver installation privilege must be restricted to administrators.	
	V-36677					Optional component installation and component repair must be prevented from using Windows Update.	

	V-36678					Device driver updates must only search managed servers not Windows Update.	
	V-15685					Users must be prevented from changing installation options.	
	V-15686					Nonadministrators must be prevented from applying vendor-signed updates.	
	V-14261					Windows must be prevented from using Windows Update to search for drivers.	
	V-21963					Windows Update must be prevented from searching for point and print drivers.	
CM-5 (6)	V-40179					Permissions for Windows installation directory must conform to minimum requirements.	
CM-6 b	V-36451					Policy must require that administrative accounts not be used with applications that access the Internet such as web browsers or with potential Internet sources such as email.	
	V-14225					Passwords for the built-in Administrator account must be changed at least annually or when a member of the administrative team leaves the organization.	
	V-14798					Directory data (outside the root DSE) of a non-public directory must be configured to prevent anonymous access.	
	V-14797					Anonymous access to the root DSE of a non-public directory must be disabled.	
	V-3337					Anonymous SID/Name translation must not be allowed.	
	V-1074					An approved DoD antivirus program must be installed and used.	
	V-14269					Mechanisms for removing zone information from file attachments must be hidden.	
	V-14268					Zone information must be preserved when saving attachments.	
	V-14270					The system must notify antivirus when file attachments are opened.	

V-1119					The system must not boot into multiple operating systems (dual-boot).	
V-1090					Caching of logon credentials must be limited.	
V-3385					The system must be configured to require case insensitivity for non-Windows subsystems.	
V-26477					Unauthorized accounts must not have the Change the time zone user right.	
V-4408					Domain controllers must be configured to allow reset of machine account passwords.	
V-1165					The computer account password must not be prevented from being reset.	
V-1154					The Ctrl+Alt+Del security attention sequence for logons must be enabled.	
V-15701					A system restore point must be created when a new device driver is installed.	
V-21961					All Direct Access traffic must be routed through the internal network.	
V-1145					Automatic logons must be disabled.	
V-4111					The system must be configured to prevent Internet Control Message Protocol (ICMP) redirects from overriding Open Shortest Path First (OSPF) generated routes.	
V-4110					The system must be configured to prevent IP source routing.	
V-11806					The system must be configured to prevent the display of the last username on the logon screen.	
V-1075					The shutdown option must not be available from the logon dialog box.	
V-3377					The system must be configured to prevent anonymous users from having the same rights as the Everyone group.	
V-1171					Ejection of removable NTFS media must be restricted to Administrators.	

V-1121					FTP servers must be configured to prevent access to the system drive.	
V-1173					The default permissions of global system objects must be increased.	
V-3469					Group Policies must be refreshed in the background if the user is logged on.	
V-4448					Group Policy objects must be reprocessed even if they have not changed.	
V-15505					The HBSS McAfee Agent must be installed.	
V-3289					Servers must have a host-based Intrusion Detection System.	
V-14232					IPSec Exemptions must be limited.	
V-21955					IPv6 source routing must be configured to the highest protection level.	
V-2378					The Kerberos user ticket lifetime must be limited to 10 hours or less.	
V-2377					The Kerberos service ticket maximum lifetime must be limited to 600 minutes or less.	
V-2376					Kerberos user logon restrictions must be enforced.	
V-2379					The Kerberos policy user ticket renewal maximum lifetime must be limited to 7 days or less.	
V-1153					The LanMan authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	
V-3381					The system must be configured to the required LDAP client signing level.	
V-3344					Local accounts with blank passwords must be restricted to prevent access from the network.	
V-15719					Users must be notified if the logon server was inaccessible and cached credentials were used.	
V-3373					The maximum age for machine account passwords must be set to requirements.	
V-15687					Users must not be presented with Privacy and Installation options on first use of Windows Media	

					Player.	
V-1168					Members of the Backup Operators group must be documented.	
V-21952					NTLM must be prevented from falling back to a Null session.	
V-1172					Users must be warned in advance of their passwords expiring.	
V-1070					Server systems must be located in a controlled access area accessible only to authorized personnel.	
V-21953					PKU2U authentication using online identities must be prevented.	
V-8327					Windows services that are critical for directory server operation must be configured for automatic startup.	
V-1120					FTP servers must be configured to prevent anonymous logons.	
V-1159					The Recovery Console option must be set to prevent automatic logon to the system.	
V-1158					The Recovery Console SET command must be disabled.	
V-15707					Remote Assistance log files must be generated.	
V-1115					The built-in administrator account must be renamed.	
V-1114					The built-in guest account must be renamed.	
V-26283					Anonymous enumeration of SAM accounts must not be allowed.	
V-15682					Attachments must be prevented from being downloaded from RSS feeds.	
V-3479					The system must be configured to use Safe DLL Search Mode.	
V-4442					The system must be configured to have password protection take effect within a limited time frame when the screen saver becomes active.	
V-1128					Security configuration tools or equivalent processes must be used to configure and maintain platforms for	

					security compliance.	
V-3382					The system must be configured to meet the minimum session security requirement for NTLM SSP-based clients.	
V-3666					The system must be configured to meet the minimum session security requirement for NTLM SSP-based servers.	
V-1157					The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	
V-15823					Software certificate installation files must be removed from a system.	
V-4446					Software certificate restriction policies must be enforced.	
V-21950					The service principal name (SPN) target name validation level must be turned off.	
V-2907					System files must be monitored for unauthorized changes.	
V-1076					System-level information must be backed up in accordance with local recovery time and recovery point objectives.	
V-8324					The time synchronization tool must be configured to enable logging of time source switching.	
V-3456					Remote Desktop Services must delete temporary folders when a session is terminated.	
V-1073					Systems must be maintained at a supported service pack level.	
V-15727					Users must be prevented from sharing files in their profiles.	
V-36658					Users with administrative privilege must be documented.	
V-36659					Users with Administrative privileges must have separate accounts for administrative duties and normal operational tasks.	

V-36662					Application account passwords must be changed at least annually or when a system administrator with knowledge of the password leaves the organization.	
V-36663					System BIOS or system controllers must have administrator accounts/passwords configured.	
V-36664					The system must not use removable media as the boot loader.	
V-36666					Policy must require that system administrators (SAs) be trained for the operating systems used by systems under their control.	
V-36670					Audit data must be reviewed on a regular basis.	
V-36671					Audit data must be retained for at least one year.	
V-36673					IP stateless autoconfiguration limits state must be enabled.	
V-36679					Early Launch Antimalware Boot-Start Driver Initialization Policy must be enabled and configured to only Good and Unknown.	
V-36680					Access to the Windows Store must be turned off.	
V-36697					Trusted app installation must be enabled to allow for signed enterprise line of business apps.	
V-36710					Automatic download of updates from the Windows Store must be turned off.	
V-36711					The Windows Store application must be turned off.	
V-43241					The setting to allow Microsoft accounts to be optional for modern style apps must be enabled (Windows 2012 R2).	
V-43245					Automatically signing in the last interactive user after a system-initiated restart must be disabled (Windows 2012 R2).	
V-15683					File Explorer shell protocol must run in protected mode.	
V-15684					Users must be notified if a web-based program attempts to install software.	

	V-57461					The system must be configured to send error reports on TCP port 1232.	
	V-42420					A host-based firewall must be installed and enabled on the system.	
	V-36733					User-level information must be backed up in accordance with local recovery time and recovery point objectives.	
	V-36735					The system must support automated patch management tools to facilitate flaw remediation.	
	V-36736					The system must query the certification authority to determine whether a public key certificate has been revoked before accepting the certificate for authentication purposes.	
	V-36772					The machine account lockout threshold must be set to 10 on systems with BitLocker enabled.	
	V-40195					System BIOS or system controllers must not allow user-level access.	
	V-40198					Members of the Backup Operators group must have separate accounts for backup duties and normal operational tasks.	
	V-40172					Backups of system-level information must be protected.	
	V-40173					System-related documentation must be backed up in accordance with local recovery time and recovery point objectives.	
	V-40204					Only the default client printer must be redirected to the Remote Desktop Session Host. (Remote Desktop Services Role).	
	V-40175					The antivirus program signature files must be kept updated.	
	V-40193					Virtual guest operating systems must be registered in a vulnerability and asset management system.	
	V-40206					The Smart Card Removal Policy service must be configured to automatic.	
CM-7 (2)	V-21973					Autoplay must be turned off for non-volume devices.	

	V-22692					The default Autorun behavior must be configured to prevent Autorun commands.	
	V-2374					Autoplay must be disabled for all drives.	
CM-7 (5) (b)	V-57637					The operating system must employ a deny-all permit-by-exception policy to allow the execution of authorized software programs.	
CM-7 a	V-26575					The 6to4 IPv6 transition technology must be disabled.	
	V-21971					The Application Compatibility Program Inventory must be prevented from collecting data and sending the information to Microsoft.	
	V-15713					Microsoft Active Protection Service membership must be disabled.	
	V-15702					An Error Report must not be sent when a generic device driver is installed.	
	V-15700					Remote access to the Plug and Play interface must be disabled for device installation.	
	V-28504					Windows must be prevented from sending an error report when a device driver requests additional software during installation.	
	V-21970					Responsiveness events must be prevented from being aggregated and sent to Microsoft.	
	V-15672					Event Viewer Events.asp links must be turned off.	
	V-26600					The Fax service must be disabled if installed.	
	V-15704					Errors in handwriting recognition on tablet PCs must not be reported to Microsoft.	
	V-16021					The Windows Help Experience Improvement Program must be disabled.	
	V-16048					Windows Help Ratings feedback must be turned off.	
	V-14260					Downloading print driver packages over HTTP must be prevented.	
	V-15674					The Internet File Association service must be turned off.	
V-26576					The IP-HTTPS IPv6 transition technology must be disabled.		

V-26577					The ISATAP IPv6 transition technology must be disabled.	
V-15722					Windows Media Digital Rights Management (DRM) must be prevented from accessing the Internet.	
V-21967					Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft must be prevented.	
V-15696					The Mapper I/O network protocol (LLTDIO) driver must be disabled.	
V-15697					The Responder network protocol driver must be disabled.	
V-15698					The configuration of wireless devices using Windows Connect Now must be disabled.	
V-15699					The Windows Connect Now wizards must be disabled.	
V-4445					Optional Subsystems must not be permitted to operate on the system.	
V-26604					The Peer Networking Identity Manager service must be disabled if installed.	
V-21964					Device metadata retrieval from the Internet must be prevented.	
V-14259					Printing over HTTP must be prevented.	
V-15667					Network Bridges must be prohibited in Windows.	
V-26605					The Simple TCP/IP Services service must be disabled if installed.	
V-3487					Necessary services must be documented to maintain a baseline to determine if additional unnecessary services have been added to a system.	
V-36681					Copying of user input methods to the system account for sign-in must be prevented.	
V-36684					Local users on domain-joined computers must not be enumerated.	
V-36687					App notifications on the lock screen must be turned off.	
V-36696					The detection of compatibility issues for applications and drivers must be turned off.	

	V-36698	Red	Yellow	Green	Grey	The use of biometrics must be disabled.	
	V-36707	Red	Yellow	Green	Grey	The Windows SmartScreen must be turned off.	
	V-36708	Red	Yellow	Green	Grey	The location feature must be turned off.	
	V-36709	Red	Yellow	Green	Grey	Basic authentication for RSS feeds over HTTP must be turned off.	
	V-43238	Red	Yellow	Green	Grey	The display of slide shows on the lock screen must be disabled (Windows 2012 R2).	
	V-43240	Red	Yellow	Green	Grey	The network selection user interface (UI) must not be displayed on the logon screen (Windows 2012 R2).	
	V-16020	Red	Yellow	Green	Grey	The Windows Customer Experience Improvement Program must be disabled.	
	V-21969	Red	Yellow	Green	Grey	Access to Windows Online Troubleshooting Service (WOTS) must be prevented.	
	V-15666	Red	Yellow	Green	Grey	Windows Peer-to-Peer networking services must be turned off.	
	V-36776	Red	Yellow	Green	Grey	Notifications from Windows Push Network Service must be turned off.	
	V-36777	Red	Yellow	Green	Grey	Toast notifications to the lock screen must be turned off.	
CM-7 b	V-26602	Red	Yellow	Green	Grey	The Microsoft FTP service must not be installed.	
	V-26606	Red	Yellow	Green	Grey	The Telnet service must be disabled if installed.	
	V-26578	Red	Yellow	Green	Grey	The Teredo IPv6 transition technology must be disabled.	
IA-11	V-15705	Red	Yellow	Green	Grey	Users must be prompted to authenticate on resume from sleep (on battery).	
	V-15706	Red	Yellow	Green	Grey	The user must be prompted to authenticate on resume from sleep (plugged in).	
	V-3376	Red	Yellow	Green	Grey	The system must be configured to prevent the storage of passwords and credentials.	
	V-3453	Red	Yellow	Green	Grey	Remote Desktop Services must always prompt a client for passwords upon connection.	
	V-14247	Red	Yellow	Green	Grey	Passwords must not be saved in the Remote Desktop Client.	

	V-14234					User Account Control approval mode for the built-in Administrator must be enabled.	
	V-14240					User Account Control must run all administrators in Admin Approval Mode enabling UAC.	
	V-14236					User Account Control must automatically deny standard user requests for elevation.	
	V-36720					The Windows Remote Management (WinRM) service must not store RunAs credentials.	
IA-2	V-7002					Accounts must require passwords.	
	V-1072					Shared user accounts must not be permitted on the system.	
IA-2 (1)	V-15488					Active directory user accounts including administrators must be configured to require the use of a Common Access Card (CAC) PIV-compliant hardware token or Alternate Logon Token (ALT) for user authentication.	
IA-2 (8)	V-2380					The computer clock synchronization tolerance must be limited to 5 minutes or less.	
IA-3	V-21951					Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	
IA-4 e	V-1112					Outdated or unused accounts must be removed from the system or disabled.	
IA-5 (1) (a)	V-1150					The built-in Windows password complexity policy must be enabled.	
	V-6836					Passwords must at a minimum be 14 characters.	
	V-36661					Policy must require application account passwords be at least 15 characters in length.	
IA-5 (1) (d)	V-1105					The minimum password age must meet requirements.	
	V-1104					The maximum password age must meet requirements.	
	V-6840					System mechanisms must be implemented to enforce automatic expiration of passwords.	
IA-5 (1) c	V-3379					The system must be configured to prevent the storage of the LAN Manager hash of passwords.	

	V-2372	Red	Yellow	Green	Grey	Reversible password encryption must be disabled.	
	V-1141	Red	Yellow	Green	Grey	Unencrypted passwords must not be sent to third-party SMB Servers.	
IA-5 (1) e	V-1107	Red	Yellow	Green	Grey	The password uniqueness must meet minimum requirements.	
IA-5 (2)	V-57639	Red	Yellow	Green	Grey	Users must be required to enter a password to access private keys stored on the computer.	
IA-6	V-36700	Red	Yellow	Green	Grey	The password reveal button must not be displayed.	
IA-7	V-21954	Red	Yellow	Green	Grey	The use of DES encryption suites must not be allowed for Kerberos encryption.	
IA-8	V-1113	Red	Yellow	Green	Grey	The built-in guest account must be disabled.	
MA-4 (6)	V-36713	Red	Yellow	Green	Grey	The Windows Remote Management (WinRM) client must not allow unencrypted traffic.	
	V-36719	Red	Yellow	Green	Grey	The Windows Remote Management (WinRM) service must not allow unencrypted traffic.	
MA-4 c	V-36712	Red	Yellow	Green	Grey	The Windows Remote Management (WinRM) client must not use Basic authentication.	
	V-36714	Red	Yellow	Green	Grey	The Windows Remote Management (WinRM) client must not use Digest authentication.	
	V-36718	Red	Yellow	Green	Grey	The Windows Remote Management (WinRM) service must not use Basic authentication.	
SC-10	V-3380	Red	Yellow	Green	Grey	The system must be configured to force users to log off when their allowed logon hours expire.	
	V-1136	Red	Yellow	Green	Grey	Users must be forcibly disconnected when their logon hours expire.	
	V-1174	Red	Yellow	Green	Grey	The amount of idle time required before suspending a session must be properly set.	
	V-14831	Red	Yellow	Green	Grey	The directory service must be configured to terminate LDAP-based network connections to the directory server after five (5) minutes of inactivity.	
	V-3457	Red	Yellow	Green	Grey	Remote Desktop Services must be configured to set a time limit for disconnected sessions.	

	V-3458					Remote Desktop Services must be configured to disconnect an idle session after the specified time period.	
SC-13	V-3383					The system must be configured to use FIPS-compliant algorithms for encryption hashing and signing.	
	V-14783					Separate NSA-approved (Type 1) cryptography must be used to protect the directory data-in-transit for directory service implementations at a classified confidentiality level when replication data traverses a network cleared to a lower level than the data.	
SC-2	V-8317					Data files owned by users must be on a different logical partition from the directory server data files.	
	V-8326					The directory server supporting (directly or indirectly) system access or resource authorization must run on a machine dedicated to that function.	
SC-28	V-57645					Systems requiring data at rest protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.	
SC-3	V-21960					Domain users must be required to elevate when setting a networks location.	
	V-14243					The system must require username and password to elevate a running application.	
	V-14235					User Account Control must at minimum prompt administrators for consent.	
	V-16008					Windows must elevate all applications in User Account Control not just signed ones.	
	V-14237					User Account Control must be configured to detect application installations and prompt for elevation.	
	V-14242					User Account Control must virtualize file and registry write failures to per-user locations.	
	V-14241					User Account Control must switch to the secure desktop when prompting for elevation.	

	V-14239					User Account Control must only elevate UIAccess applications that are installed in secure locations.	
	V-15991					UIAccess applications must not be allowed to prompt for elevation without using the secure desktop.	
SC-4	V-3338					Named pipes that can be accessed anonymously must be configured with limited values on domain controllers.	
	V-6834					Anonymous access to Named Pipes and Shares must be restricted.	
	V-3340					Network shares that can be accessed anonymously must not be allowed.	
	V-1093					Anonymous enumeration of shares must be restricted.	
	V-3245					File shares must limit access to data on a system.	
	V-3470					The system must be configured to prevent unsolicited remote assistance offers.	
	V-3343					Solicited Remote Assistance must not be allowed.	
	V-3339					Unauthorized remotely accessible registry paths must not be configured.	
	V-4443					Unauthorized remotely accessible registry paths and sub-paths must not be configured.	
	V-3378					The system must be configured to use the Classic security model.	
	V-14249					Local drives must be prevented from sharing with Remote Desktop Session Hosts. (Remote Desktop Services Role).	
SC-5	V-4112					The system must be configured to disable the Internet Router Discovery Protocol (IRDP).	
	V-21956					IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	
	V-4116					The system must be configured to ignore NetBIOS name release requests except from WINS servers.	
	V-4113					The system must be configured to limit how often keep-alive packets are sent.	

	V-4438					The system must limit how many times unacknowledged TCP data is retransmitted.	
	V-15718					Turning off File Explorer heap termination on corruption must be disabled.	
SC-5 (2)	V-14228					Auditing the Access of Global System Objects must be turned off.	
	V-14229					Auditing of Backup and Restore Privileges must be turned off.	
SC-8	V-6831					Outgoing secure channel traffic must be encrypted or signed.	
	V-1163					Outgoing secure channel traffic must be encrypted when possible.	
	V-4407					Domain controllers must require LDAP access signing.	
	V-1164					Outgoing secure channel traffic must be signed when possible.	
	V-6832					The Windows SMB client must be configured to always perform SMB packet signing.	
	V-1166					The Windows SMB client must be enabled to perform SMB packet signing when possible.	
	V-6833					The Windows SMB server must be configured to always perform SMB packet signing.	
	V-1162					The Windows SMB server must perform SMB packet signing when possible.	
	V-3374					The system must be configured to require a strong session key.	
	V-57459					The system must be configured to use SSL to forward error reports.	
SC-8 (2)	V-57641				Protection methods such as TLS encrypted VPNs or IPSEC must be implemented if the data owner has a strict requirement for ensuring data integrity and confidentiality is maintained at every step of the data transfer and handling process.		
SI-11 a	V-56511				The Windows Error Reporting Service must be running and configured to start automatically.		

	V-57457					The system must be configured to store error reports locally on the system or in the enclave and not send them to Microsoft.	
	V-57463					The system must be configured to archive error reports.	
	V-57479					The system must be configured to permit the default consent levels of Windows Error Reporting to override any other consent policy setting.	
SI-11 b	V-57455					The system must be configured to prevent the display of error messages to the user.	
SI-16	V-21980					Explorer Data Execution Prevention must be enabled.	
SI-2 (2)	V-36734					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).	