

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



**Technical Assessment Guide for  
Windows 7 Operating System**

**July 2016**

Revision  
Log

<b>Date</b>	<b>Revision</b>	<b>Description of Change</b>
2016FEB24	1.0	Initial Draft
2016MAY08	1.2	Updated to include DRAFT artifacts
2016JUN08	1.3	Updated formatting, Changed ODAA to NAO
2016JUL06	1.4	Updated content to address remote scanning

**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\_7\_VIR27\_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.



## 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-17 (1)	V-14248					Users must be prevented from connecting using Remote Desktop Services.	
	V-26540					The system will be configured to audit Logon/Logoff -> Logoff successes.	
	V-26541					The system will be configured to audit Logon/Logoff -> Logon successes.	
	V-26542					The system will be configured to audit Logon/Logoff -> Logon failures.	
AC-17 (2)	V-3454				Remote Desktop Services is not configured with the client connection encryption set to the required level.		
AC-2 (4)	V-26535					The system will be configured to audit Account Management -> Security Group Management successes.	
	V-26536					The system will be configured to audit Account Management -> Security Group Management failures.	
	V-26537					The system will be configured to audit Account Management -> User Account Management successes.	
	V-26538					The system will be configured to audit Account Management -> User Account Management failures.	

<b>AC-3</b>	V-1155					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 administrator accounts on domain systems and unauthenticated access on all systems.	
	V-26470					Unauthorized accounts must not have the Access this computer from the network user right.	
	V-26472					Unauthorized accounts will 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-26483					The Deny log on as a batch job 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-26484					The Deny log on as a service user right on workstations must be configured to prevent access from highly privileged domain accounts on domain systems. No other groups or accounts must be assigned this right.	
	V-26485					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-26486					The Deny log on through Remote Desktop Services user right on workstations must prevent all access if RDS is not used by the organization. If RDS is used it must be configured to prevent access from highly privileged domain accounts and local administrator accounts on domain systems and unauthenticated access on all systems.	
	V-26495					Unauthorized accounts must not have the Log on as a batch job user right.	
	V-28285					Unauthorized users must not have the Log on as a service User Right.	
<b>AC-6 (10)</b>	V-1102					The Act as part of the operating system user right must be granted to no accounts.	
	V-18010					Unauthorized accounts must not have the Debug programs user right.	

V-26471					Unauthorized accounts must not have the Adjust memory quotas for a process user right.	
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-26487					Unauthorized accounts must not have the Enable computer and user accounts to be trusted for delegation user right.	
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-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-26502				Unauthorized accounts must not have the Remove computer from docking station 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-26505				Unauthorized accounts must not have the Shut down the system user right.	
	V-26506				Unauthorized accounts must not have the Take ownership of files or other objects user right.	
<b>AC-7 a</b>	V-1097				The system must lockout accounts after 3 invalid logon attempts within a specified time period.	
	V-1098				The period of time before the invalid logon counter is reset must be configured to at least 60 minutes.	
<b>AC-7 b</b>	V-1099				The account lockout duration must be configured to require an administrator to unlock an account.	
<b>AC-8 a</b>	V-1089				The required legal notice must be configured to display before console logon.	
	V-26359				The Windows dialog box title for the legal banner must be configured.	
<b>AU-12 a</b>	V-14230				Audit policy using subcategories is enabled.	
<b>AU-12 c</b>	V-26529				The system will be configured to audit Account Logon -> Credential Validation successes.	
	V-26530				The system will be configured to audit Account Logon -> Credential Validation failures.	
	V-26531				The system will be configured to audit Account Management -> Computer Account Management successes.	

V-26532					The system will be configured to audit Account Management -> Computer Account Management failures.	
V-26533					The system will be configured to audit Account Management -> Other Account Management Events successes.	
V-26534					The system will be configured to audit Account Management -> Other Account Management Events failures.	
V-26539					The system will be configured to audit Detailed Tracking -> Process Creation successes.	
V-26543					The system will be configured to audit Logon/Logoff -> Special Logon successes.	
V-26544					The system will be configured to audit Object Access -> File System failures.	
V-26545					The system will be configured to audit Object Access -> Registry failures.	
V-26546					The system will be configured to audit Policy Change -> Audit Policy Change successes.	
V-26547					The system will be configured to audit Policy Change -> Audit Policy Change failures.	
V-26548					The system will be configured to audit Policy Change -> Authentication Policy Change successes.	
V-26549					The system will be configured to audit Privilege Use -> Sensitive Privilege Use successes.	
V-26550					The system will be configured to audit Privilege Use -> Sensitive Privilege Use failures.	
V-26551					The system will be configured to audit System -> IPSec Driver successes.	
V-26552					The system will be configured to audit System -> IPSec Driver failures.	
V-26553					The system will be configured to audit System -> Security State Change successes.	
V-26554					The system will be configured to audit System -> Security State Change failures.	
V-26555					The system will be configured to audit System -> Security System Extension successes.	
V-26556					The system will be configured to audit System -> Security System Extension failures.	

	V-26557					The system will be configured to audit System -> System Integrity successes.	
	V-26558					The system will be configured to audit System -> System Integrity failures.	
<b>AU-4</b>	V-26579					The Application event log must be configured to a minimum size requirement.	
	V-26580					The Security event log must be configured to a minimum size requirement.	
	V-26581					The Setup event log must be configured to a minimum size requirement.	
	V-26582					The System event log must be configured to a minimum size requirement.	
<b>AU-5 a</b>	V-4108					The system must generate an audit event when the audit log reaches a percentage of full threshold.	
<b>AU-9</b>	V-26496					Unauthorized accounts must not have the Manage auditing and security log user right.	
<b>CM-11 (2)</b>	V-1151					Print driver installation privilege must be restricted to administrators.	
	V-14261					Windows is prevented from using Windows Update to search for drivers.	
	V-15685					Prevent users from changing Windows installer options.	
	V-15686					Prevent users from installing vendor signed updates.	
	V-15703					Users will not be prompted to search Windows Update for device drivers.	
	V-15724					Unsigned gadgets must not be installed.	
	V-15725					The More Gadgets link must be disabled.	
	V-15726					User-installed gadgets must be turned off.	
	V-21963					Prevent searching Windows Update for point and print drivers.	
	V-21965					Prevent Windows Update for device driver search	
	V-21974					Turn off downloading of game updates.	
	V-3480					Media Player must be configured to prevent automatic checking for updates.	
	V-34974					The Windows Installer Always install with elevated privileges must be disabled.	
<b>CM-6 b</b>	V-1073					Systems must be at supported service pack (SP) or release levels.	

V-1075	Red	Yellow	Green	Grey	The system allows shutdown from the logon dialog box.	
V-1084	Red	Yellow	Green	Grey	System pagefile is cleared upon shutdown.	
V-1085	Red	Yellow	Green	Grey	Floppy media devices are not allocated upon user logon.	
V-1090	Red	Yellow	Green	Grey	Caching of logon credentials must be limited.	
V-1114	Red	Yellow	Green	Grey	The built-in guest account must be renamed.	
V-1115	Red	Yellow	Green	Grey	The built-in administrator account must be renamed.	
V-1145	Red	Yellow	Green	Grey	Automatic logons must be disabled.	
V-1153	Red	Yellow	Green	Grey	The Lan Manager authentication level must be set to send NTLMv2 response only and to refuse LM and NTLM.	
V-1154	Red	Yellow	Green	Grey	Ctrl+Alt+Del security attention sequence is disabled.	
V-1157	Red	Yellow	Green	Grey	The Smart Card removal option must be configured to Force Logoff or Lock Workstation.	
V-1158	Red	Yellow	Green	Grey	The Recovery Console SET command must be disabled.	
V-1159	Red	Yellow	Green	Grey	The Recovery Console option is set to permit automatic logon to the system.	
V-1165	Red	Yellow	Green	Grey	The computer account password is prevented from being reset.	
V-1171	Red	Yellow	Green	Grey	Ejection of removable NTFS media is not restricted to administrators.	
V-1172	Red	Yellow	Green	Grey	Users are not warned in advance that their passwords will expire.	
V-1173	Red	Yellow	Green	Grey	The default permissions of global system objects are not increased.	
V-11806	Red	Yellow	Green	Grey	The system is configured to allow the display of the last user name on the logon screen.	
V-14231	Red	Yellow	Green	Grey	The system must be configured to hide the computer from the browse list.	
V-14232	Red	Yellow	Green	Grey	IPSec exemptions are limited.	
V-14262	Red	Yellow	Green	Grey	IPv6 must be disabled until a deliberate transition strategy has been implemented.	
V-15680	Red	Yellow	Green	Grey	The classic logon screen must be required for user logons.	
V-15682	Red	Yellow	Green	Grey	Attachments must be prevented from being downloaded from RSS feeds.	
V-15683	Red	Yellow	Green	Grey	Shell protocol runs in protected mode.	
V-15684	Red	Yellow	Green	Grey	IE security prompt is enabled for web-based installations.	

V-15687	Red	Yellow	Green	Grey	Prevent first use dialog boxes for Windows Media Player from displaying for users.	
V-15701	Red	Yellow	Green	Grey	Enable restore points for device driver installations.	
V-15707	Red	Yellow	Green	Grey	Session logging for Remote Assistance is enabled.	
V-15709	Red	Yellow	Green	Grey	Disable Game Explorer information downloads.	
V-15719	Red	Yellow	Green	Grey	Users must be notified if the logon server was inaccessible and cached credentials were used.	
V-15823	Red	Yellow	Green	Grey	Software certificate installation files must be removed from a system.	
V-17373	Red	Yellow	Green	Grey	Secure Removable Media – CD-ROM	
V-21950	Red	Yellow	Green	Grey	The service principal name (SPN) target name validation level must be configured to Accept if provided by client.	
V-21952	Red	Yellow	Green	Grey	NTLM must be prevented from falling back to a Null session.	
V-21953	Red	Yellow	Green	Grey	PKU2U authentication using online identities must be prevented.	
V-21955	Red	Yellow	Green	Grey	IPv6 source routing must be configured to highest protection.	
V-21961	Red	Yellow	Green	Grey	Route all Direct Access traffic through internal network.	
V-26283	Red	Yellow	Green	Grey	Anonymous enumeration of SAM accounts will not be allowed.	
V-26477	Red	Yellow	Green	Grey	Unauthorized accounts must not have the Change the time zone user right.	
V-3344	Red	Yellow	Green	Grey	The use of local accounts with blank passwords is not restricted to console logons only.	
V-3373	Red	Yellow	Green	Grey	The maximum age for machine account passwords is not set to requirements.	
V-3375	Red	Yellow	Green	Grey	Domain Controller authentication is not required to unlock the workstation.	
V-3377	Red	Yellow	Green	Grey	The system is configured to give anonymous users Everyone rights.	
V-3381	Red	Yellow	Green	Grey	The system is not configured to recommended LDAP client signing requirements.	
V-3382	Red	Yellow	Green	Grey	The system must be configured to meet the minimum session security requirement for NTLM SSP based clients.	

	V-3385					The system must be configured to require case insensitivity for non-Windows subsystems.	
	V-3455					Remote Desktop Services must be configured to use session-specific temporary folders.	
	V-3456					Remote Desktop Services is not configured to delete temporary folders.	
	V-3479					The system is not configured to use Safe DLL search mode.	
	V-3666					The system must be configured to meet the minimum session security requirement for NTLM SSP based servers.	
	V-39137					The Enhanced Mitigation Experience Toolkit (EMET) v5.x or later must be installed on the system.	
	V-4110					The system is configured to allow IP source routing.	
	V-4111					The system is configured to redirect ICMP.	
	V-4442					This check verifies that Windows is configured to have password protection take effect within a limited time frame when the screen saver becomes active.	
	V-4448					Group Policy objects are not reprocessed if they have not changed.	
	V-45589					A group must be defined on domain systems to include all local administrator accounts.	
<b>CM-7 (2)</b>	V-21973					Turn off autoplay for non-volume devices.	
	V-22692					The default autorun behavior must be configured to prevent autorun commands.	
	V-2374					The system is configured to autoplay removable media.	
<b>CM-7 a</b>	V-14256					Web publishing and online ordering wizards prevented from downloading list of providers.	
	V-14259					Prevent printing over HTTP.	
	V-14260					Computer prevented from downloading print driver packages over HTTP.	
	V-15666					Turn off Windows Peer-to-Peer Networking Services.	
	V-15667					Prohibit Network Bridge in Windows.	
	V-15672					Event Viewer events.asp links are available.	
	V-15674					Disable Internet File Association Service.	
	V-15676					Order Prints Online is blocked.	

V-15696	Red	Yellow	Green	Grey	Disable the Mapper I/O Driver.	
V-15697	Red	Yellow	Green	Grey	Disable the Responder network protocol driver.	
V-15698	Red	Yellow	Green	Grey	The configuration of wireless devices using Windows Connect Now will be disabled.	
V-15699	Red	Yellow	Green	Grey	Disable the Windows Connect Now wizards.	
V-15700	Red	Yellow	Green	Grey	Disable remote access to the plug and play interface.	
V-15702	Red	Yellow	Green	Grey	A Windows error report is not sent when a generic driver is installed.	
V-15704	Red	Yellow	Green	Grey	Handwriting recognition error reports (Tablet PCs) are not sent to Microsoft.	
V-15711	Red	Yellow	Green	Grey	Turn off indexing of encrypted files.	
V-15712	Red	Yellow	Green	Grey	Indexing of mail items in Exchange folders when Outlook is running in uncached mode must be turned off.	
V-15713	Red	Yellow	Green	Grey	Turn off Windows Defender SpyNet reporting.	
V-15722	Red	Yellow	Green	Grey	Prevent Windows Media Digital Rights Management (DRM) from accessing the Internet.	
V-16006	Red	Yellow	Green	Grey	The system must not have unnecessary features installed.	
V-16020	Red	Yellow	Green	Grey	Windows Customer Experience Improvement Program is disabled.	
V-21964	Red	Yellow	Green	Grey	Device metadata retrieval from the Internet must be prevented.	
V-21966	Red	Yellow	Green	Grey	Prevent handwriting personalization data sharing with Microsoft.	
V-21967	Red	Yellow	Green	Grey	Prevent Microsoft Support Diagnostic Tool (MSDT) interactive communication with Microsoft.	
V-21969	Red	Yellow	Green	Grey	Prevent access to Windows Online Troubleshooting Service (WOTS).	
V-21970	Red	Yellow	Green	Grey	Disable Performance PerfTrack.	
V-21971	Red	Yellow	Green	Grey	Prevent the Application Compatibility Program Inventory from collecting data and sending the information to Microsoft.	
V-21975	Red	Yellow	Green	Grey	Prevent the system from joining a homegroup.	
V-21978	Red	Yellow	Green	Grey	Windows Anytime Upgrade is not disabled.	
V-26575	Red	Yellow	Green	Grey	The 6to4 IPv6 transition technology will be disabled.	
V-26576	Red	Yellow	Green	Grey	The IP-HTTPS IPv6 transition technology will be disabled.	

	V-26577	Red	Yellow	Green	Grey	The ISATAP IPv6 transition technology will be disabled.	
	V-3347	Red	Yellow	Green	Grey	Internet Information System (IIS) or its subcomponents must not be installed on a workstation.	
<b>CM-7 b</b>	V-26578	Red	Yellow	Green	Grey	The Teredo IPv6 transition technology will be disabled.	
<b>IA-11</b>	V-14234	Red	Yellow	Green	Grey	User Account Control for the built In admin runs in Admin Approval Mode	
	V-14236	Red	Yellow	Green	Grey	User Account Control is configured for the appropriate elevation prompt for standard users.	
	V-14240	Red	Yellow	Green	Grey	User Account Control - Run all admins in Admin Approval Mode.	
	V-14247	Red	Yellow	Green	Grey	Terminal Services / Remote Desktop Service - Prevent password saving in the Remote Desktop Client.	
	V-15705	Red	Yellow	Green	Grey	Password is required on resume from sleep (on battery).	
	V-15706	Red	Yellow	Green	Grey	Password is required on resume from sleep (plugged in).	
	V-3376	Red	Yellow	Green	Grey	The system is configured to permit storage of passwords and credentials.	
	V-3453	Red	Yellow	Green	Grey	Remote Desktop Services is not configured to always prompt a client for passwords upon connection.	
<b>IA-2</b>	V-16047	Red	Yellow	Green	Grey	The built-in administrator account must be disabled.	
<b>IA-3</b>	V-21951	Red	Yellow	Green	Grey	Services using Local System that use Negotiate when reverting to NTLM authentication must use the computer identity vs. authenticating anonymously.	
<b>IA-3 (1)</b>	V-14253	Red	Yellow	Green	Grey	Restrict unauthenticated RPC clients.	
	V-14254	Red	Yellow	Green	Grey	Client computers required to authenticate for RPC communication.	
<b>IA-5 (1) (a)</b>	V-1150	Red	Yellow	Green	Grey	The built-in Microsoft password filter is not enabled.	
	V-6836	Red	Yellow	Green	Grey	For systems utilizing a logon ID as the individual identifier passwords must be a minimum of 14 characters in length.	
<b>IA-5 (1) (c)</b>	V-1141	Red	Yellow	Green	Grey	Unencrypted passwords must not be sent to third-party SMB Servers.	
	V-2372	Red	Yellow	Green	Grey	Reversible password encryption must be disabled.	
	V-3379	Red	Yellow	Green	Grey	The system is configured to store the LAN Manager hash of the password in the SAM.	
<b>IA-5 (1) (d)</b>	V-1104	Red	Yellow	Green	Grey	The maximum password age must be configured to 60 days or less.	

	V-1105					The minimum password age must be configured to at least 1 day.	
<b>IA-5 (1) (e)</b>	V-1107					The password history must be configured to 24 passwords.	
<b>IA-5 (2) (a)</b>	V-15671					Root certificates will not be updated automatically from Microsoft.	
	V-32272					The DoD Root Certificate must be installed.	
	V-32273					The External CA Root Certificate must be installed.	
	V-32274					The DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate must be installed.	
	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.	
<b>IA-7</b>	V-21954					The use of DES encryption suites must not be allowed for Kerberos encryption.	
<b>IA-8</b>	V-1113					The built-in guest account must be disabled.	
<b>SC-10</b>	V-1136					Users are not forcibly disconnected when logon hours expire.	
	V-1174					The amount of idle time required before suspending a session must be properly set.	
	V-3380					The system must be configured to force users to log off when their allowed logon hours expire.	
	V-3457					Remote Desktop Services is not configured to set a time limit for disconnected sessions.	
	V-3458					Remote Desktop Services idle session time limit does not meet the requirement.	
<b>SC-13</b>	V-3383					The system is not configured to use FIPS compliant algorithms for encryption hashing and signing.	
<b>SC-3</b>	V-14235					User Account Control is configured for the appropriate elevation prompt for administrators	
	V-14237					User Account Control is configured to detect application installations.	
	V-14239					User Account Control - Elevate UIAccess applications that are in secure locations.	
	V-14241					User Account Control - Switch to secure desktop.	
	V-14242					User Account Control - Non UAC compliant applications run in virtualized file and registry entries.	

	V-14243	Red	Yellow	Green	Grey	Require username and password to elevate a running application.	
	V-16008	Red	Yellow	Green	Grey	UAC - All application are elevated.	
	V-21960	Red	Yellow	Green	Grey	Require domain users to elevate when setting a network's location.	
	V-36439	Red	Yellow	Green	Grey	Local administrator accounts must have their privileged token filtered to prevent elevated privileges from being used over the network on domain systems.	
<b>SC-4</b>	V-1093	Red	Yellow	Green	Grey	Anonymous enumeration of shares must be restricted.	
	V-14249	Red	Yellow	Green	Grey	Terminal Services / Remote Desktop Services - Local drives prevented from sharing with Terminal Servers/Remote Session Hosts.	
	V-3338	Red	Yellow	Green	Grey	Named pipes that can be accessed anonymously must be configured to contain no values.	
	V-3339	Red	Yellow	Green	Grey	Unauthorized remotely accessible registry paths must not be configured.	
	V-3340	Red	Yellow	Green	Grey	Unauthorized shares can be accessed anonymously.	
	V-3343	Red	Yellow	Green	Grey	Solicited Remote Assistance is allowed.	
	V-3378	Red	Yellow	Green	Grey	The system is not configured to use the Classic security model.	
	V-3470	Red	Yellow	Green	Grey	The system must be configured to prevent unsolicited remote assistance offers.	
	V-4443	Red	Yellow	Green	Grey	Unauthorized remotely accessible registry paths and sub-paths must not be configured.	
	V-6834	Red	Yellow	Green	Grey	Named pipes and shares can be accessed anonymously.	
<b>SC-5</b>	V-15718	Red	Yellow	Green	Grey	Disable heap termination on corruption in Windows Explorer.	
	V-21956	Red	Yellow	Green	Grey	IPv6 TCP data retransmissions must be configured to prevent resources from becoming exhausted.	
	V-4112	Red	Yellow	Green	Grey	The system is configured to detect and configure default gateway addresses.	
	V-4113	Red	Yellow	Green	Grey	The system is configured for a greater keep-alive time than recommended.	
	V-4116	Red	Yellow	Green	Grey	The system must be configured to ignore NetBIOS name release requests except from WINS servers.	
	V-4438	Red	Yellow	Green	Grey	The system must limit how many times unacknowledged TCP data is retransmitted.	

<b>SC-5 (2)</b>	V-14228	Red	Yellow	Green	Grey	Auditing Access of Global System Objects must be turned off.	
	V-14229	Red	Yellow	Green	Grey	Audit of backup and restore privileges is not turned off.	
<b>SC-8 (1)</b>	V-1162	Red	Yellow	Green	Grey	The Windows SMB server is not enabled to perform SMB packet signing when possible.	
	V-1163	Red	Yellow	Green	Grey	Outgoing secure channel traffic is not encrypted when possible.	
	V-1164	Red	Yellow	Green	Grey	Outgoing secure channel traffic is not signed when possible.	
	V-1166	Red	Yellow	Green	Grey	The Windows SMB client is not enabled to perform SMB packet signing when possible.	
	V-3374	Red	Yellow	Green	Grey	The system is not configured to require a strong session key.	
	V-6831	Red	Yellow	Green	Grey	Outgoing secure channel traffic is not encrypted or signed.	
	V-6832	Red	Yellow	Green	Grey	The Windows SMB client is not enabled to always perform SMB packet signing.	
	V-6833	Red	Yellow	Green	Grey	The Windows SMB server is not enabled to always perform SMB packet signing.	
<b>SI-11 a</b>	V-15714	Red	Yellow	Green	Grey	The system must be configured to save Error Reporting events and messages to the system event log.	
	V-15715	Red	Yellow	Green	Grey	The system must be configured to generate error reports.	
	V-15717	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-56511	Red	Yellow	Green	Grey	The Windows Error Reporting Service must be running and configured to start automatically.	
	V-57463	Red	Yellow	Green	Grey	The system must be configured to archive error reports.	
	V-57465	Red	Yellow	Green	Grey	The system must be configured to store all data in the error report archive.	
	V-57467	Red	Yellow	Green	Grey	The maximum number of error reports to archive on a system must be configured to 100 or greater.	
	V-57469	Red	Yellow	Green	Grey	The system must be configured to queue error reports until a local or DOD-wide collector is available.	
V-57471	Red	Yellow	Green	Grey	The system must be configured to add all error reports to the queue.		

	V-57473				The maximum number of error reports to queue on a system must be configured to 50 or greater.	
	V-57475				The system must be configured to attempt to forward queued error reports once a day.	
	V-57477				The system must be configured to automatically consent to send all data requested by a local or DOD-wide error collection site.	
	V-57479				The system must be configured to permit the default consent levels of Windows Error Reporting to override any other consent policy setting.	
<b>SI-11 b</b>	V-57455				The system must be configured to prevent the display of error messages to the user.	
<b>SI-16</b>	V-21980				Explorer Data Execution Prevention is disabled.	
	V-36701				The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomization (ASLR) must be enabled and configured to Application Opt In.	
	V-36702				The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer must be enabled.	
	V-36703				The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Recommended Software must be enabled.	
	V-36704				The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software must be enabled.	
	V-36705				The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) must be enabled and configured to at least Application Opt Out.	
	V-36706				The Enhanced Mitigation Experience Toolkit (EMET) system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be configured to Application Opt Out.	

