MICROSOFT WINDOWS 10 STIG
REVISION HISTORY

Version 2, Release 9

15 May 2024

Developed by DISA for the DOD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R9	- Windows 10 STIG, V2R8	- WN10-00-000025 - Rule ID updated due to changes in content management system. - WN10-00-000030, WN10-00-000031, WN10-00-000032 - Elevated to CAT I. - WN10-00-000035 - Updated Check to remove "This is applicable to unclassified systems; for other systems, this is Not Applicable." - WN10-00-000040 - Updated Check and Fix text with OS version number. - WN10-00-000095 - Removed ICACLS for C:\ S-1-15-3******. - WN10-AU-000585 - Added missing path level in Check and Fix. - WN10-SO-000280 - Updated Check text to include nondomain joined systems.	15 May 2024
V2R8	- Windows 10 STIG, V2R7	- WN10-00-000040 - Updated check and fix with OS versions and support levels. - WN10-00-000095 - Updated check text with new SID. - WN10-00-000395 - Added requirement to disable port proxying. - WN10-AU-000585 - Added requirement to enable command line process auditing for failures. - WN10-CC-000205 - Updated the group ID in the check and fix. - WN10-PK-000005 - Updated certificate type DoD CA 6. - WN10-SO-000035, WN10-SO-000040, WN10-SO-000045, WN10-SO-000060, WN10-SO-000100, WN10-SO-000120 - Rule IDs updated due to changes in content management system. - WN10-SO-000251 - Updated wording in check text. - WN10-SO-000280 - Updated check text to include settings.	09 November 2023
V2R7	- Windows 10 STIG, V2R6	- WN10-SO-000280 - Updated Vul Discussion and Fix text.	07 June 2023
V2R6	- Windows 10 STIG, V2R5	- WN10-00-000035 - Revised AppLocker Deployment Guide link in Check and Fix; replaced “whitelist” with “allowlist”.	11 May 2023

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- WN10-00-000085 - Revised Check to note that for standalone or nondomain-joined systems, this is Not Applicable. - WN10-00-000250 - Revised Rule title from "should" to "must"; revised Check to state "If the system is NOT a nonpersistent VM, this is Not Applicable." - WN10-CC-000075 - Revised finding statement in Check to reflect "Virtualization-based Security Services Running". - WN10-CC-000391 - Added a requirement to disable Internet Explorer. - WN10-PK-000005, WN10-PK-000015, WN10-PK-000020 - Revised Check and Fix to reflect current/updated certificates and added PKI link for DOD certificates to Fix. - WN10-SO-000251 - Revised Check to state "If the system is a member of a domain, this is Not Applicable." - WN10-SO-000280 - Revised Discussion wording to "not generally used and its password may not be changed...". - Some Rule IDs updated due to changes in content management system. - Addressed issues of STIG style compliance.	
V2R5	- Windows 10 STIG, V2R4	- WN10-00-000005, WN10-CC-000050 - Changed wording in the Check text from "standalone" to "standalone or nondomain-joined". - WN10-00-000010, WN10-CC-000115, WN10-CC-000130, WN10-CC-000206, WN10-UR-000075, WN10-UR-000080 - Changed wording in the Check and Fix text from "standalone" to "standalone or nondomain-joined". - WN10-00-000030, WN10-00-000031, WN10-00-000032, WN10-PK-000005, WN10-PK-000015 - Corrected CCIs. - WN10-00-000040 - Updated Check and Fix text regarding versioning. - WN10-CC-000055 - In Check and Fix text, set Minimize simultaneous connections to Enabled; set Minimize Policy Options to 3, Prevent Wi-Fi while on Ethernet.	14 November 2022

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Some Rule IDs and CCIs updated due to minor changes in content management system.	
V2R4	- Windows 10 STIG, V2R3	- WN10-00-000030, WN10-00-000031, WN10-00-000032 - Changed Check text from "WVD" to "AVD" for Azure Virtual Desktop. - WN10-00-000040 - Updated Check and Fix: Windows servicing levels need to be updated. - WN10-AU-000550 - Removed requirement. - WN10-AU-000570 - Updated Fix text: Object Access >> "Audit Detailed File Share" with "Failure" selected. - WN10-CC-000007 - Updated Check and Fix registry label and settings with Value Name: Value; Value Data: Deny. - WN10-CC-000050, WN10-SO-000280 - Rule ID changed in data management system. - WN10-CC-000080 - Added requirement back to STIG per government and SHB. - WN10-CC-000327 - Rule ID changed due to reparenting SRG ID. - WN10-PK-000005, WN10-PK-000015 - Removed all deprecated DOD Root CA 2 references. - WN10-SO-000251 - Changed Check text: If the system is "not" a member of a domain, this is Not Applicable.	31 May 2022
V2R3	- Windows 10 STIG, V2R2	- WN10-00-000025 - Replaced HBSS references with Endpoint Security Solution. - WN10-00-000045 - Changed HBSS to Endpoint Security Solution in Check; in Fix, clarified that anti-virus software must be in use. - WN10-00-000160 - Updated Check with current Vul IDs V-220730 and V-220731. - WN10-00-000165, WN10-00-000170 - Updated Check with current Vul ID V-220729. - WN10-CC-000050, WN10-CC-000327 - Added requirement back into STIG after database issue. - WN10-CC-000204 - Revised Vul reference in Check to V-220834. - WN10-EP-000020, WN10-EP-000030, WN10-EP-000040, WN10-EP-000050, WN10-EP-000060, WN10-EP-000070, WN10-EP-000080,	01 November 2021

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		WN10-EP-000090, WN10-EP-000100, WN10-EP-000110, WN10-EP-000120, WN10-EP-000130, WN10-EP-000140, WN10-EP-000150, WN10-EP-000160, WN10-EP-000170, WN10-EP-000180, WN10-EP-000190, WN10-EP-000200, WN10-EP-000220, WN10-EP-000230, WN10-EP-000240, WN10-EP-000250, WN10-EP-000260, WN10-EP-000270, WN10-EP-000280, WN10-EP-000290, WN10-EP-000300 - Removed Exploit Protection requirements. Settings for EMET deprecated by Microsoft. - WN10-SO-000251 - Removed fix text note regarding supplemental guidance; document does not exist. - WN10-SO-000280- Updated Check/Fix to highly recommend use of LAPS, and AO can approve other solutions.	
V2R2	- Windows 10 STIG, V2R1	- WN10-00-000015 - Corrected grammar in finding statement. - WN10-00-000025 - Removed HBSS wording. Updated Check and Fix and added Note section. - WN10-00-000040 - Updated new and removed older OS versions in Check. - WN10-00-000045 - In Check text, added PowerShell fix checks for Windows Defender for third-party AV. In Fix text, specified use of Windows Defender or a third-party antivirus option. - WN10-CC-000204 - Updated Vul ID reference in Check. - WN10-CC-000345 - Added temporary Security Override Guidance for configuration for Office 365 DOD tenants. - WN10-CC-000385 - Revised wording in rule title for clarity.	04 May 2021
V2R1	- Windows 10 STIG, V1R21	- DISA migrated the STIG to a new content management system, which renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number from V1R21 to V2R1.	13 November 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- WN10-00-000030 - Added text, "For WVD implementations with no data at rest, this is NA." - WN10-00-000031 - In Check: Added registry settings for BitLocker Network unlock; added text "For virtual desktop implementations (VDIs) in which the virtual desktop instance is deleted or refreshed upon logoff, this is NA" and "For WVD implementations with no data at rest, this is NA". - WN10-00-000032 - Added Check text: "For virtual desktop implementations (VDIs) in which the virtual desktop instance is deleted or refreshed upon logoff, this is NA" and "For WVD implementations with no data at rest, this is NA". - WN10-00-000040 - Updated support dates for current Semi-Annual Channel versions. - WN10-CC-000327 - Added requirement that PowerShell Transcription must be enabled on Windows 10. - WN10-CC-000340 - Removed requirement that OneDrive must only allow synchronizing of accounts for DOD organization instances. - WN10-EP-000200 - Removed "override" from check text and revised fix text. - WN10-EP-000210 - Removed requirement (added to Microsoft OneDrive STIG). - WN10-PK-000005, WN10-PK-000010, WN10-PK-000015, WN10-PK-000020 - Removed "If an expired certificate ("Valid to" date)" wording. - WN10-UC-000005 - Removed requirement that the use of personal accounts for OneDrive synchronization must be disabled.	
V1R21	- Windows 10 STIG, V1R20	- V-100093 - Added new requirement for the OS. - V-99555 - Changing wording from "built in" to "enabled local" for the Administrator account.	24 April 2020
V1R20	- Windows 10 STIG, V1R19	- V-63323 - Upgraded severity level from CAT III to CAT II.	27 January 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63349 - Revised required version to Windows Version 1709 or greater. - V-63441 - Removed requirement to configure the system to audit Account Management - Other Account Management Events successes. - V-63455 - Removed requirement to configure the system to audit Logon/Logoff - Account Lockout successes. - V-63475 – Removed requirement to configure the system to audit Policy Change - Audit Policy Change failures. - V-63495 - Removed requirement for Audit IPsec Driver Audit Success. - V-63587 - Changed wording. "If an expired certificate is found, this is a finding." - V-63589 - Changed wording. "If an expired certificate is found, this is a finding." - V-63599 - Changed Windows 10 Credential Guard requirement severity to CAT I. - V-63607 - Revised rule title to prevent boot drivers, not just those identified as bad, and revised configuration instructions. - V-63705 - Removed requirement to allow InPrivate browsing Disabled. - V-63707 - Remove requirement for Microsoft network client: Digitally sign communications (if server agrees) Success. - V-63723 - Removed requirement for SMB packet signing. - V-63763 - Remove requirement for Network security: Allow Local System to use computer identity for NTLM. - V-63887 - Removed requirement that generate security audits user right must only be assigned to Local Service and Network Service. - V-63891 - Removed requirement to increase scheduling priority. - V-72769 - Changed Check Text "This is NA if the system does not have Bluetooth, or if Bluetooth is turned off per the organizations policy." - V-74415 - Removed requirement to allow clearing browsing data on exit.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-77189 - Changed Exploit Protection setting for Windows 10 Acrobat.exe. - V-77191 - Changed Exploit Protection setting for Windows 10 AcroRd32.exe. - V-77195 - Changed Exploit Protection setting for Windows 10 Chrome.exe. - V-77201 - Changed Exploit Protection setting for Windows 10 Excel.exe. - V-77205 - Changed Exploit Protection setting for Windows 10 Firefox.exe. - V-77209 - Changed Exploit Protection setting for Windows 10 FLTLDR.exe. - V-77213 - Changed Exploit Protection setting for Windows 10 Groove.exe. - V-77217 - Changed Exploit Protection setting for Windows 10 Iexplorer.exe. - V-77221 - Changed Exploit Protection setting for Windows 10 Infopath.exe. - V-77223 - Changed Exploit Protection setting for Windows 10 Java.exe. - V-77227 - Changed Exploit Protection setting for Windows 10 Lync.exe. - V-77231 - Changed Exploit Protection setting for Windows 10 Msaccess.exe. - V-77233 - Changed Exploit Protection setting for Windows 10 MSpub.exe. - V-77235 - Changed Exploit Protection setting for Windows 10 OneDrive.exe. - V-77239 - Changed Exploit Protection setting for Windows 10 OIS.exe. - V-77243 - Changed Exploit Protection setting for Windows 10 Outlook.exe. - V-77247 - Changed Exploit Protection setting for Windows 10 Powerpnt.exe. - V-77249 - Changed Exploit Protection setting for Windows 10 Pptview.exe. - V-77255 - Changed Exploit Protection setting for Windows 10 Visio.exe. - V-77259 - Changed Exploit Protection setting for Windows 10 Vpreview.exe. - V-77263 - Changed Exploit Protection setting for Windows 10 Winword.exe. - V-77267 - Changed Exploit Protection setting for Windows 10 Wmplayer.exe.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-77269 - Changed Exploit Protection setting for Windows 10 Wordpad.exe. - V-88203 - Revised to WN10-CC-000340 to create a unique STIGID. - V-94861 - Added registry path to check text: Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE - V-99541 - Added requirement to audit other Logon/Logoff Events - Failures. - V-99543 - Added requirement to audit other Logon/Logoff Events - Successes. - V-99545 - Added requirement to audit Detailed File Share - Failures. - V-99547 - Added requirement to audit MPSSVC Rule-Level Policy Change - Successes. - V-99549 - Added requirement to audit MPSSVC Rule-Level Policy Change - Failures. - V-99551 - Added requirement to audit Other Policy Change Events - Successes. - V-99553 - Added requirement to audit Other Policy Change Events - Failures. - V-99555 - Added requirement to change passwords for built-in local Administrator account at least every 60 days. - V-99557 - Added requirement to enable Windows 10 Kernel (Direct Memory Access) DMA Protection. - V-99559 - Added requirement to disable the convenience PIN for Windows 10. - V-99561 - Added requirement to configure Windows Ink Workspace to disallow access above the lock. - V-99563 - Added requirement to configure Window 10 to prevent users from receiving suggestions for third-party or additional applications. - Revised DOD_EP file in Supporting Files folder.	
V1R19	- Windows 10 STIG, V1R18	V-88203 - Group Title: Rename from WN10-CC-000340 to WN10-CC-000360.	25 October 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R18	- Windows 10 STIG, V1R17	- V-63323 - Added note to requirement regarding severity level upgrade January 2020. - V-63337 - Updated to allow other FullDisk Encryption (FDE) applications in lieu of BitLocker. - V-63349 - Updated to include details for v1903. - V-63393 - Added note to requirement regarding Adobe Preflight certificate files. - V-63403 - Updated requirement with GPO path for v1703 and higher. - V-63533 - Updated to allow permissions for "APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES". - V-63537 - Updated to allow permissions for "APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES". - V-63541 - Updated to allow permissions for "APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES". - V-63595 - Added note to requirement regarding severity level upgrade January 2020. - V-63599 - Added note to requirement regarding severity level upgrade January 2020. - V-63603 - Removed Virtualization-based Protection of Code Integrity requirement. - V-63875 - Corrected typo in the Check Text and Fix Text making the Enterprise Admins group and the Domain Admins group plural. - V-63879 - Corrected typo in the Check Text making the Enterprise Admins group and the Domain Admins group plural. - V-63891 - Updated to allow assignment to "Window Manager\Window Manager Group". - V-68819 - Updated requirement to remove extra space from registry path. - V-74413 - Updated requirement to remove extra space from registry path. - V-74415 - Updated requirement to remove extra space from registry path.	26 July 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-74719 - Updated requirement to verify the Secondary Logon service is not running. - Added note to the following requirements to match the case for the filename if the PowerShell command does not garner results. V-77189, V-77191, V-77195, V-77201, V-77205, V-77209, V-77213, V-77217, V-77221, V-77223, V-77227, V-77231, V-77233, V-77235, V-77239, V-77243, V-77245, V-77247, V-77249, V-77255, V-77259, V-77263, V-77267, V-77269 - V-94859 - Added to new requirement for BitLocker PIN. - V-94861 - Added to new requirement for BitLocker PIN length. - Removed EMET references from the Overview document.	
V1R17	- Windows 10 STIG, V1R16	- V-63343 - Removed vendor specific references and functions not covered by HBSS. - V-63349 - Updated requirement to require at least v1703. - V-63365 - Updated requirement to allow authorized accounts. - V-63587 - Replaced FBCA Cross-Certificate Removal Tool with InstallRoot Application in Fix Text. Added new certificate. Removed expired certificates. - V-63589 - Replaced FBCA Cross-Certificate Removal Tool with InstallRoot Application in Fix Text. Removed expired certificate. - V-63593 - Updated requirement with a note detailing new default permissions in later versions of Windows 10. - V-63685 - Updated for v1607 semi-annual channel version (SAC) end of support; changed to note v1607 LTSB. - V-63699 - Updated for v1607 semi-annual channel version (SAC) end of support. - V-63701 - Updated for v1607 semi-annual channel version (SAC) end of support. - V-63713 - Updated for v1607 semi-annual channel version (SAC) end of support.	24 May 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63721 - Updated for v1607 semi-annual channel version (SAC) end of support; changed to note v1607 LTSB. - V-70637 - Corrected PowerShell command syntax in Check Text. - V-74415 - Removed v1703 applicability note. - V-74417 - Removed v1703 applicability note, added LTSC\LTSB non-applicability statement. - V-74699 - Removed v1703 applicability note, added LTSC\LTSB non-applicability statement. - V-94719 - Added new requirement to prevent apps from being activated by voice when the system is locked	
V1R16	- Windows 10 STIG, V1R15	- V-63337 - Updated Full Disk encryption requirement to direct sites to use BitLocker on all Windows 10 information systems (including SIPRNET).	25 January 2019
V1R15	- Windows 10 STIG, V1R14	- V-63337 - Changed requirement to a CAT II, expanded mobile system text. - V-63349 - Updated based on Microsoft extension of support for previous releases. Added V1809 release. - V-63361 - Removed exception note referencing AD admin platforms. - V-63455 - Corrected group policy path. - V-63499 - Corrected group policy path. - V-63503 - Corrected group policy path. - V-63569 - Added v1507 LTSB non-applicability statement. - V-63591 - Added note related to v1507 LTSB configuration. Updated to note this is NA as of v1803. - V-63599 - Added note for v1507 LTSB group policy selection options. - V-63659 - Added LTSC\LTSB non-applicability statement. - V-63669 - Updated to clarify allowed configuration is 900 seconds or less, excluding 0. - V-63677 - Added v1507 LTSB non-applicability statement. Changed note regarding versions prior to v1703 to address v1607 specifically.	15 November 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63683 - Updated to allow Enhanced telemetry when limited to support Windows Analytics. - V-63715 - Removed by DOD Consensus as it has minimal effect on Workstations. - V-63725 - Replaced with V-82137, User setting that prevents personal OneDrive accounts. - V-63753 - Removed by DOD Consensus due to functional issues caused by setting. - V-63851 - Removed exception note referencing AD admin platforms. - V-63871 - Updated reference from AD admin platforms to Privileged Access Workstations (PAWs). - V-63877 - Updated reference from AD admin platforms to Privileged Access Workstations (PAWs). - V-63879 - Updated reference from AD admin platforms to Privileged Access Workstations (PAWs). - V-71759 - Corrected group policy path. - V-71771 - Added v1507 LTSB non-applicability statement. - V-74415 - Added LTSC\LTSB non-applicability statement. - V-77025 - Removed by DOD Consensus, as users do not have this privilege. - V-77083 - Added VDI exception consistent with other VBS supporting requirements. - V-77085 - Added VDI exception consistent with other VBS supporting requirements. - V-77095 - Corrected XML in Fix to enforce configuration. - V-82137 - Added new requirement to prevent use of personal OneDrive accounts, replaces V-63725. - V-82139 - Added requirement to prevent certificate error overrides in Microsoft Edge. - V-82145 - Added requirement to limit Enhanced telemetry when enabled. - V-88203 - Added requirement to restrict OneDrive syncing to organizational instance.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R14	- Windows 10 STIG, V1R13	- V-63345 - Updated link to referenced NSA document. - V-63367 - Updated local account exceptions, vary depending on Windows 10 version. - V-63579 - Updated with additional certificate. Added certificate expiration dates for reference. - V-63583 - Added certificate expiration dates for reference. - V-63587 - Added certificate expiration dates for reference. - V-63589 - Updated with additional certificate. Added certificate expiration dates for reference. - V-68849 - Removed references to EMET, no longer supported by Microsoft as of 31 July 2018. - V-77083 - Raised severity of UEFI requirement from CAT III to CAT II. Removed older system compatibility note. - Corrected typo of DEP to DOD in reference to the XML file for the following: - V-77091, V-77095, V-77097, V-77101, V-77103. **Windows 10 Benchmark, V1R12**: - V-63533 - Updated Application event log permissions check to address issue with Java-based scan engines. - V-63537 - Updated Security event log permissions check to address issue with Java-based scan engines. - V-63541 - Updated System event log permissions check to address issue with Java-based scan engines. - V-63579 - Updated DOD Root CA OVAL content to include additional certificate. - V-63589 - Updated DOD CCEB Interoperability Root CA OVAL content to include additional certificate. - V-63669 - Updated Machine Inactivity OVAL content to ensure a value of "0" will result in a finding. - V-68849 - Updated Structured Exception Handling Overwrite Protection (SEHOP) OVAL content removing EMET portion in	27 July 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		conjunction with the update to the manual STIG.	
V1R13	- Windows 10 STIG, V1R12	- V-63349 - Updated servicing level requirement for v1511 EOL as well as changes in support for later versions. - V-63395 - Removed HBSS McAfee Agent requirement, addressed by product STIG. - V-63439 - Removed Other Account Management failure event audit requirement as NA. - V-63443 - Removed Security Group Management failure event audit requirement as NA. - V-63471 - Added exception to removable storage auditing for virtual machines. - V-63473 - Added exception to removable storage auditing for virtual machines. - V-63511 - Removed Security System Extension failure event audit requirement as NA. - V-63523 - Updated to increase minimum Security event log size to 1G. - V-63595 - Removed standalone non-applicability statement. - V-63603 - Updated Virtualization-based protection of code integrity requirement for v1511 EOL; added v1507 LTSB note. Removed standalone non-applicability statement. - V-63637 - Removed requirement as providing minimal benefit. - V-63685 - Updated Windows Defender SmartScreen for Explorer requirement for v1511 EOL, added v1507 LTSB note, added applicability statement for unclassified only. - V-63699 - Updated Windows Defender SmartScreen for Edge websites requirement for v1511 EOL; added applicability statement for unclassified only as well as being NA for LTSC\B versions. - V-63701 - Updated Windows Defender SmartScreen for Edge files requirement for v1511 EOL; added applicability statement for unclassified only as well as being NA for LTSC\B versions.	27 April 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63705 - Updated Microsoft Edge InPrivate browsing requirement for v1511 EOL, as well as being NA for LTSC\B versions. - V-63709 - Updated Microsoft Edge password manager requirement for v1511 EOL, as well as being NA for LTSC\B versions. - V-63713 - Updated Windows Defender SmartScreen for Edge requirement for v1511 EOL; added applicability statement for unclassified only as well as being NA for LTSC\B versions. - V-63717 - Updated Windows Hello for Business TPM requirement for v1511 EOL; added v1507 LTSB note. - V-63721 - Updated minimum PIN length requirement for v1511 EOL; added v1507 LTSB note. - V-63799 - Removed as providing minimal benefit. - V-63813 - Removed as providing minimal benefit. - V-63835 - Removed; function provided by another requirement. - V-63837 - Removed; function provided by another requirement. - V-65681 - Updated Delivery Optimization requirement for v1511 EOL, and v1507 LTSB note. - V-71769 - Updated Security Account Manager remote calls requirement for v1511 EOL, as well as being NA for v1507 LTSB version. - V-73811 - Removed antivirus signature requirement, addressed by AV product STIGs. **Exploit Protection Requirements** - Added applicability statement for unclassified only to the following: - V-77025, V-77189, V-77191, V-77195, V-77201, V-77209, V-77213, V-77217, V-77221, V-77223, V-77227, V-77231, V-77233, V-77239, V-77243, V-77245, V-77247, V-77249, V-77255, V-77259, V-77263, V-77267, V-77269.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- In addition to the unclassified applicability statement, the mitigations for the following were updated: - V-77205, V-77235. - In addition to the unclassified applicability statement, added clarification of the default configuration and added enforcement option to the following: - V-77091, V-77095, V-77097, V-77101, V-77103. - The DOD_EP XML file was updated to version 2 with changes to mitigations for OneDrive and Firefox. **Windows 10 Benchmark, V1R11**: - V-63349 - Updated OVAL due to v1511 end of support. - V-63395 - Disabled OVAL due to STIG rule removal. - V-63439 - Disabled OVAL due to STIG rule removal. - V-63443 - Disabled OVAL due to STIG rule removal. - V-63511 - Disabled OVAL due to STIG rule removal. - V-63523 - Updated OVAL due to increase in minimum Security event log size to 1G. - V-63637 - Disabled OVAL due to STIG rule removal. - V-63685 - Updated OVAL due to V1511 end of support. - V-63799 - Disabled OVAL due to STIG rule removal. - V-63813 - Disabled OVAL due to STIG rule removal. - V-65681 - Updated OVAL due to v1511 end of support. - V-68849 - Updated OVAL content to address ACAS error in OVAL variable object when EMET is not installed. - V-71769 - Updated OVAL due to v1511 end of support.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R12	- Windows 10 STIG, V1R11	- V-63845 - Updated to note allowed exception to access computer from the network user right. - V-78129 - Added requirement that administrator accounts must not be used for Internet access consistent with other Windows STIGs. **Windows 10 STIG Overview**: - Updated Section 3.5 Windows Apps for removing apps from a user profile. **Windows 10 Benchmark, V1R10**: - V-63377 - Modified to verify the status of the IIS features using wmi57 tests in lieu of registry tests. - V-70639 - Updated OVAL content for the SMBv1 Protocol requirement. - V-74719 - Updated comment to correctly reference the "Secondary Logon" service. - V-74723 - Updated OVAL content for the SMBv1 Server requirement. - V-74725 - Updated OVAL content for the SMBv1 Client requirement. - V-76505 - Added OVAL to identify orphaned SIDs.	26 January 2018
V1R11	- Windows 10 STIG, V1R10	**The STIG has been updated for the latest release of Windows 10, v1709**: - V-63349 - Updated to note Microsoft's continued support of v1511. Added projected end of support dates for current versions. **Removed EMET requirements, replaced by built-in Exploit Protection for v1709**: V-63379, V-63387, V-63391, V-63397, V-63401, V-63407, V-63411, V-63417, V-63425, V-63433. - V-68845 - Removed reference to being an alternate to the EMET requirement for DEP. - V-68849 - Updated alternate SEHOP requirement to be applicable prior to v1709 of Windows 10. **Added the following Exploit Protection requirements**:	31 October 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-77025 - Prevent Exploit Protection changes from being made in Windows Defender Security Center. V-77091 - Enforce Exploit Protection system level mitigation for Data Execution Prevention (DEP). V-77095 - Enforce Exploit Protection system level mitigation for Bottom-Up Address Space Layout Randomization (Bottom-Up ASLR). V-77097 - Enforce Exploit Protection system level mitigation for Control Flow Guard (CFG). V-77101 - Enforce Exploit Protection system level mitigation for Structured Exception Handling Overwrite Protection (SEHOP). V-77103 - Enforce Exploit Protection system level mitigation for Heap Integrity. V-77189 - Exploit Protection application level mitigations for Acrobat.exe. V-77191 - Exploit Protection application level mitigations for AcroRd32.exe. V-77195 - Exploit Protection application level mitigations for chrome.exe. V-77201 - Exploit Protection application level mitigations for EXCEL.exe. V-77205 - Exploit Protection application level mitigations for firefox.exe. V-77209 - Exploit Protection application level mitigations for FLTLDR.exe. V-77213 - Exploit Protection application level mitigations for GROOVE.exe. V-77217 - Exploit Protection application level mitigations for iexplore.exe. V-77221 - Exploit Protection application level mitigations for INFOPATH.exe. V-77223 - Exploit Protection application level mitigations for java*.exe. V-77227 - Exploit Protection application level mitigations for lync.exe. V-77231 - Exploit Protection application level mitigations for MSACCESS.exe. V-77233 - Exploit Protection application level mitigations for MSPUB.exe. V-77239 - Exploit Protection application level mitigations for OIS.exe.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-77235 - Exploit Protection application level mitigations for OneDrive.exe. V-77243 - Exploit Protection application level mitigations for OUTLOOK.exe. V-77245 - Exploit Protection application level mitigations for plugin-container.exe. V-77247 - Exploit Protection application level mitigations for POWERPNT.exe. V-77249 - Exploit Protection application level mitigations for PPTVIEW.exe. V-77255 - Exploit Protection application level mitigations for VISIO.exe. V-77259 - Exploit Protection application level mitigations for VPREVIEW.exe. V-77263 - Exploit Protection application level mitigations for WINWORD.exe. V-77267 - Exploit Protection application level mitigations for wmplayer.exe. V-77269 - Exploit Protection application level mitigations for wordpad.exe. - V-63675 - Removed short version of banner text as NA. - V-63579 - Clarified details apply to unclassified systems, refers to PKE documentation for other systems. - V-63351 - Removed specific antivirus product referenced. - V-76505 - Added requirement for unresolved SIDs found on user rights. - V-63365 - Added note for allowed exceptions regarding Hyper-V. - V-63865 - Added note for allowed exceptions regarding Hyper-V. - V-63373 - Updated for default permission changes after v1511. - V-77083 - Added requirement to verify system firmware is UEFI. - V-77085 - Added requirement to verify Secure Boot is enabled. **Windows 10 STIG Overview**: - Updated section 3.6 of for change in terminology on feature releases.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Added section 3.8 Windows Defender Exploit Protection. **Windows 10 Benchmark, V1R9**: - Removed EMET requirements: V-63379, V-63387, V-63391, V-63397, V-63401, V-63407, V-63411, V-63417, V-63425, V-63433. - V-77025 - Added OVAL for new requirement.	
V1R10	- Windows 10 STIG, V1R9	- Added section on Cortana to the STIG Overview. - The SecGuide custom admin template files have been updated to include additional configuration settings. - V-63349 - Added note v1511 of Windows 10 will become unsupported on 10 October 2017. - V-63319 - Clarified that 64-bit version of Windows 10 Enterprise is required. - V-63405 - Updated account lockout duration to 15 minutes or greater. - V-63595 - Updated Fix to include title for policy options selections. - V-63599 - Removed option for Credential Guard to be enabled without UEFI lock. - V-63641 - Removed untrusted font blocking requirement. - V-63677 - Updated for policy name change in v1703. - V-63685 - Updated for name, policy path and registry changes in v1703. - V-63691 - Corrected Fix to include "Not Configured" option. - V-63699 - Updated for name and policy path change in v1703. - V-63701 - Updated for name and policy path change in v1703. - V-63713 - Updated for name and policy path change in v1703. - V-63721 - Updated for policy path change in v1703. - V-63845 - Updated requirement to allow Remote Desktop Users to have user right.	27 June 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-68849 - Updated Fix to use custom admin template instead of direct registry update. - V-70639 - Updated requirement to allow alternate method to disable SMBv1. - V-74409 - Added requirement to audit Other Object Access Events - Failures. - V-74411 - Added requirement to audit Other Object Access Events - Successes. - V-74413 - Added requirement to define ECC Curve Order. - V-74415 - Added requirement to prevent clearing browser data when Edge closes. - V-74417 - Added requirement to prevent game recording. - V-74699 - Added requirement to enable remote host delegation of non-exportable credentials. - V-74719 - Added requirement to disable the secondary logon service. - V-74721 - Added requirement to audit File Share - Successes. - V-74723 - Added requirement to allow alternate method to disable SMBv1 server. - V-74725 - Added requirement to allow alternate method to disable SMBv1 client. - V-75027 - Added requirement to audit File Share - Failures. **Windows 10 Benchmark, V1R8**: - V-63319 - Update to check for 64-bit version of Windows 10 Enterprise. - V-63405 - Updated account lockout duration to 15 minutes or greater. - V-63641 - Removed untrusted font blocking requirement. - V-63685 - Updated for changes in v1703. - V-63845 - Updated requirement to allow Remote Desktop Users to have user right. - V-70639 - Updated requirement to allow alternate method to disable SMBv1. - V-74409 - Added requirement to audit Other Object Access Events - Failures. - V-74411 - Added requirement to audit Other Object Access Events - Successes.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-74415 - Added requirement to prevent clearing browser data when Edge closes. - V-74417 - Added requirement to prevent game recording. - V-74699 - Added requirement to enable remote host delegation of non-exportable credentials. - V-74719 - Added requirement to disable the secondary logon service. - V-74721 - Added requirement to audit File Share - Successes. - V-74723 - Added requirement to allow alternate method to disable SMBv1 server. - V-74725 - Added requirement to allow alternate method to disable SMBv1 client. - V-75027 - Added requirement to audit File Share - Failures.	
V1R9	- Windows 10 STIG, V1R8	- V-63319 - Changed terminology regarding authentication information protected. - V-63323 - Changed terminology regarding authentication information protected. - V-63351 - Moved antivirus signature to separate requirement (V-73811). - V-63353 - Clarified with regard to EFI partitions. - V-63395 - Clarified versions of service being verified. - V-63581 - Expanded Vulnerability Discussion on effect of setting. - V-63599 - Changed terminology regarding authentication information protected. - V-71769 - Updated to note setting is applicable starting with v1607 release. - V-73811 - Moved antivirus signature to separate requirement (previously part of V-63351). Updated to require configuration of daily checks as well as a maximum age of one week. **Updated the following to note changes between Windows 10 versions**: V-63603, V-63685, V-63699, V-63701, V-63705, V-63709, V-63713, V-63717, V-63721, V-65681.	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Windows 10 Benchmark, V1R7: - V-63685 - Updated to account for changes between Windows 10 versions. - V-65681 - Updated to account for changes between Windows 10 versions. - V-71769 - Updated to include a Windows version check. - Added new XCCDF profile to disable EMET checks where they are not applicable.	
V1R8	- Windows 10 STIG, V1R7	- Removed Section 3.1 of the Overview document, which previously addressed the STIG requirement to be at the latest version of Windows 10. - Overview Section 3.6 - Added paragraph regarding STIG changes between Windows 10 versions. - V-63587 - Updated expired certificate with replacement. - V-71767 - Removed requirement to be at version 1607 of Windows 10. - V-72765 - Added requirement to turn disable Bluetooth unless organization approved. - V-72767 - Added requirement to turn off Bluetooth when not in use. - V-72769 - Added requirement for Bluetooth notifications when devices attempt to connect.	11 January 2017
V1R7	- Windows 10 STIG, V1R6	This update is based on the Windows 10 update, version 1607. **Removed Error Reporting requirements**: V-63437, V-63461, V-63489, V-63493, V-63497, V-63505, V-63521, V-63525, V-63535, V-63539, V-63543, V-63547, V-63557, V-63561, V-63565, V-63571, V-63575. **The following were removed by DOD Consensus**: V-63551, V-63573, V-63613, V-63631, V-63655, V-63693, V-63727, V-63735, V-63761, V-63809, V-63849, V-63929, V-63937, V-63957, V-68821. **Added the following new requirements**:	08 November 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-71759 - Account Lockout Failure audits. - V-71761 - Authorization Policy Change Success audits. - V-71763 - Disable WDigest. - V-71765 - Disable Internet connection sharing. - V-71767 - Windows 10 version 1607 required. - V-71769 - SAM RPC restrictions. - V-71771 - Disable Microsoft consumer experiences. - V-72329 - Remove Run as different user. **Changed Group policy names or paths for the following with Windows 10 version 1607**: V-63699, V-63701, V-63705, V-63709, V-63713, V-63717, V-63721. - V-63349 - Removed reference to initial release of the STIG. - V-63597 - Added custom administrative template for configuration. Changed STIG ID from WN10-RG-000010. - V-63599 - Updated to allow configuration without UEFI lock. - V-63603 - Updated to allow configuration without UEFI lock. - V-63683 - Updated to allow "Basic" telemetry. - V-63685 - Group policy configuration updated to "Enabled" without additional options. - V-63691 - Updated to allowed default configuration. - V-63841 - Updated to allowed default configuration. - V-63455 - Corrected Fix text. - V-63457 - Corrected Fix text. **Windows 10 Benchmark, V1R5** **Disabled the following rules in OVAL in conjunction with the removal of the requirement from the manual STIG**: V-63437, V-63461, V-63489, V-63493, V-63497, V-63505, V-63521, V-63525, V-63535, V-63539, V-63543, V-63547, V-63557, V-63561, V-63565, V-63571, V-63575, V-63551, V-63631, V-63655,	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-63735, V-63809, V-63849, V-63929, V-63937, V-63957, V-68821. **Updated OVAL for the following content in conjunction with modifications to the requirement in the manual STIG**: V-63683, V-63685, V-63691. **Added new OVAL for the following content in conjunction with new requirement added to the manual STIG**: V-71759, V-71761, V-71763, V-71765, V-71767, V-71769, V-71771, V-72329. - V-63873 - Updated OVAL content to only require Enterprise Admin and Domain Admin groups be assigned the user right.	
V1R6	- Windows 10 STIG, V1R5	- V-63327 - Removed firmware related requirement as outside of OS scope. - V-63331 - Removed firmware related requirement as outside of OS scope. - V-63395 - Updated for v5 of McAfee agent. - V-63521 - Clarified requirement for location of Windows Error Reporting data. - V-63529 - Removed Windows Error Reporting port requirement, not security related. - V-63579 - Updated PKE related requirement with current certificates. - V-63583 - Updated PKE related requirement with current certificates. - V-63587 - Updated PKE related requirement with current certificates. - V-63589 - Updated PKE related requirement with current certificates. - V-70637 - Added requirement to disable legacy feature PowerShell 2.0. - V-70639 - Added requirement to disable legacy feature SMB 1.0. **Windows 10 Benchmark, V1R4**: - V-63395 - Updated OVAL to include the new McAfee Agent Service name. - V-63529 - Disabled the rule in OVAL, removed from STIG.	28 October 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63579 - Updated OVAL to reference current certificates. - V-63583 - Updated OVAL to reference current certificates. - V-63587 - Updated OVAL to reference current certificates. - V-63589 - Updated OVAL to reference current certificates. - V-63601 - Added new OVAL content. - V-63611 - Added new OVAL content. - V-63619 - Added new OVAL content. - V-63625 - Added new OVAL content. - V-63699 - Updated OVAL to work with LTSB versions. - V-63701 - Updated OVAL to work with LTSB versions. - V-63705 - Updated OVAL to work with LTSB versions. - V-63709 - Updated OVAL to work with LTSB versions. - V-63713 - Updated OVAL to work with LTSB versions. - V-68817 - Added new OVAL content. - V-68819 - Added new OVAL content. - V-68821 - Added new OVAL content. - V-70637 - Added new OVAL content. - V-70639 - Added new OVAL content.	
V1R5	- Windows 10 STIG, V1R4	- V-63323 - Changed to CAT III. - V-63345 - Changed to CAT II.	22 July 2016
V1R4	- Windows 10 STIG, V1R3	- Added section on Virtualization Based Security Hypervisor Code Integrity to the STIG Overview. - V-63327 - Clarified with regard to virtual machines. - V-63331 - Clarified with regard to virtual machines. - V-63415 - Clarified with regard to selection of 24 for password history. - V-63345 - Updated PowerShell query used to determine AppLocker effective policy. - V-63349 - Clarified with regard to LTSB version.	08 June 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63595 - Updated to allow for either Secure Boot or Secure Boot with DMA Protections. - V-68817 - Added command line audit requirement. - V-68819 - Added PowerShell audit requirement. - V-68821 - Added PowerShell audit requirement. The following requirements related to Credential Guard and Virtualization Based Security have been changed to CAT IIIs. They will be re-evaluated in the future: V-63599, V-63595, V-63603. - Alternate CAT I requirements have been added to the STIG to replace EMET if it has not been installed. - V-68845 Alternate DEP configuration. - V-68849 Alternate SEHOP configuration. - Existing EMET requirements are NA if the alternate settings are configured. - V-63379, V-63387, V-63391, V-63397, V-63401, V-63407, V-63411, V-63417, V-63425, V-63433. **Windows 10 Benchmark, V1R3**: - Added SCAP 1.2 Validation Fixes to Windows 10 Benchmark. - V-63319 - Modified the OVAL content to work with Windows 10 LTSB. - V-63349 - Modified the OVAL content to work with Windows 10 LTSB. - V-63431 - Added new OVAL content. - V-63435 - Added new OVAL content. - V-63439 - Added OVAL for Windows 10 Audit Policy. - V-63441 - Added new OVAL content. - V-63443 - Added OVAL for Windows 10 Audit Policy. - V-63445 - Added new OVAL content. - V-63447 - Added OVAL for Windows 10 Audit Policy.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63449 - Added OVAL for Windows 10 Audit Policy. - V-63453 - Added OVAL for Windows 10 Audit Policy. - V-63455 - Added new OVAL content. - V-63459 - Added OVAL for Windows 10 Audit Policy. - V-63463 - Added OVAL for Windows 10 Audit Policy. - V-63467 - Added new OVAL content. - V-63469 - Added new OVAL content. - V-63475 - Added OVAL for Windows 10 Audit Policy. - V-63479 - Added OVAL for Windows 10 Audit Policy. - V-63481 - Added OVAL for Windows 10 Audit Policy. - V-63483 - Added OVAL for Windows 10 Audit Policy. - V-63487 - Added new OVAL content. - V-63491 - Added new OVAL content. - V-63495 - Added OVAL for Windows 10 Audit Policy. - V-63499 - Added new OVAL content. - V-63503 - Added new OVAL content. - V-63507 - Added OVAL for Windows 10 Audit Policy. - V-63511 - Added new OVAL content. - V-63513 - Added OVAL for Windows 10 Audit Policy. - V-63515 - Added new OVAL content. - V-63517 - Added new OVAL content. - V-63683 - Modified the OVAL content to work with Windows 10 LTSB. - V-63717 - Removed OVAL content due to VDI exception. - V-63871 - Added OVAL for Windows 10 User Rights. - V-63873 - Added OVAL for Windows 10 User Rights. - V-63875 - Added OVAL for Windows 10 User Rights. - V-63877 - Added OVAL for Windows 10 User Rights.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-63879 - Added OVAL for Windows 10 User Rights. - V-68845 - Added OVAL. - V-68849 - Added OVAL. - Existing EMET requirements are NA if the alternate settings are configured. - V-63379, V-63387, V-63391, V-63397, V-63401, V-63407, V-63411, V-63417, V-63425, V-63433.	
V1R3	- Windows 10 STIG, V1R2	- V-63351 - Corrected data entry error in Check and Severity Override. - V-63387 - Updated for change in EMET 5.5. - V-63391 - Updated for change in EMET 5.5. - V-63397 - Updated for change in EMET 5.5. - V-63475 - Corrected typo in Fix. - V-63479 - Corrected typo in Fix. - V-63551 - Corrected data entry error in Check and Severity Override. - V-63871 - Clarified references to local accounts instead of local administrator accounts. - V-63879 - Clarified references to local accounts instead of local administrator accounts. - V-65681 - Added requirement to prevent Windows Update from using peer systems on the Internet. **Windows 10 Benchmark, V1R2**: - V-65681 - Added OVAL. - V-63387 - Updated for change in EMET 5.5. - V-63391 - Updated for change in EMET 5.5. - V-63397 - Updated for change in EMET 5.5.	22 April 2016
V1R2	- Windows 10 STIG, V1R1	- Virtual Desktop Implementation section added to the STIG Overview. **The following requirements were clarified with regard to Virtual Desktop Implementations**: - V-63323, V-63595, V-63599, V-63603, V-63717.	01 February 2016