WINDOWS 10 STIG
REVISION HISTORY

Version 1, Release 12

26 January 2018

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V1R12	- Windows 10 STIG	- 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 - Modifiedto 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	**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.	31 October 2017

REVISION HISTORY				
Revision Number	**Document Revised**	**Description of Change**		**Release Date**
		Added the following Exploit Protection requirements: 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 system level for Structured Exception Handling Overwrite Protection (SEHOP). V-77103 - Enforce Exploit Protection system system level 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.		

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		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. 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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	- 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.	27 June 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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:**	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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	- 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.	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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 **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	- 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.	11 January 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-72769 - Added requirement for Bluetooth notifications when devices attempt to connect.	
V1R7	- Windows 10 STIG	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**: - 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.	08 November 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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, 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	- V-63327 - Removed firmware related requirement as outside of OS scope.	28 October 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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	- V-63323 - Changed to CAT III. - V-63345 - Changed to CAT II.	22 July 2016
V1R4	- Windows 10 STIG	- 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. - 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.	08 June 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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.	

UNCLASSIFIED

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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	- V-63351 - Corrected data entry error in Check and Severity Override.	22 April 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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.	
V1R2	- Windows 10 STIG	- 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