WINDOWS 8/8.1 STIG
REVISION HISTORY

Version 1, Release 20

26 January 2018

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R20	- Windows 8/ 8.1 STIG	- V-26470 - Updated to note allowed exception to access computer from the network user right. - V-73519 - Corrected reference to Windows 10. - V-73523 - Corrected reference to Windows 10. **Windows 8/8.1 Benchmark, V1R21:** - V-3347 - Modified to verify the status of the IIS features using wmi57 tests in lieu of registry tests.	26 January 2018
V1R19	- Windows 8/ 8.1 STIG	- The SecGuide custom admin template files have been updated to include additional configuration settings. - V-1074 - Removed specific antivirus product referenced. - V-1089 - Removed short version of banner text as NA. - V-32272 - Clarified details apply to unclassified systems, refers to PKE documentation for other systems. - V-73519 - Added as alternate method for disabling SMBv1 server. - V-73523 - Added as alternate method for disabling SMBv1 client. - V-73805 - Updated to allow alternate method for disabling SMBv1. - V-75915 - Added requirement for unresolved SIDs found on user rights. - Removed the following user rights requirements that provide minimal security benefit. V-26475 - Bypass traverse checking. V-26477 - Change the time zone. V-26502 - Remove computer from docking station. V-26505 - Shut down the system. V-28285 - Log on as a service. **Windows 8/8.1 Benchmark, V1R20:** - Removed OVAL content for the following as requirement has been removed from the STIG V-26475, V-26477, V-26502, V-26505, V-28285.	27 October 2017

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- V-73519 - Added OVAL content to the benchmark. - V-73523 - Added OVAL content to the benchmark. - V-73805 - Updated the OVAL content for SMBv1 Protocol requirement to allow a combination of the V-73519 and V-73523 fixes to close the requirement.	
V1R18	- Windows 8/ 8.1 STIG	- V-1098 - Updated reset account lockout counter to 15 minutes or greater. - V-1099 - Updated account lockout duration to 15 minutes or greater. - V-36770 - Updated Fix to use custom admin template instead of direct registry update. **Windows 8/8.1 Benchmark, V1R19:** - V-1098 - Updated OVAL content for reset account lockout counter change to 15 minutes or greater. - V-1099 - Updated OVAL content for account lockout duration change to 15 minutes. - V-1152 - Enabled Winreg registry check previously disabled due to an SCC bug. - V-26070 - Added OVAL to check permissions on Winlogon registry key.	28 July 2017
V1R17	- Windows 8/ 8.1 STIG	- V-1074 - Moved antivirus signature to separate requirement (V-40175). Changed STIG ID. - V-1152 - Clarified permissions must be at least as restrictive as defaults. - V-15505 - Clarified versions of service being verified. - V-26070 - Clarified permissions must be at least as restrictive as defaults. - V-36674 - Expanded Vulnerability Discussion on effect of setting. - V-40175 - Moved antivirus signature to separate requirement (previously part of V-1074). Updated to require configuration of daily checks as well as a maximum age of one week. - V-73805 - Added requirement to disable Server Message Block (SMB) v1.	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Windows 8/8.1 Benchmark, V1R18: - V-15505 - Added OVAL to check if one of the supported versions of the McAfee agents is installed and running. - V-73805 - Added OVAL to check if the SMB 1.0/CIFS File Sharing Support feature is disabled. - Added new XCCDF profile to disable EMET checks where they are not applicable.	
V1R16	- Windows 8/ 8.1 STIG	- V-14236 - Changed User Account Control standard user elevation to automatically deny. - V-32274 - Updated expired certificate with replacement. - V-72753 - Added requirement to disable WDigest. - Removed Error Reporting requirements: V-15714, V-15715, V-15717, V-56511, V-57453, V-57455, V-57457, V-57459, V-57463, V-57465, V-57467, V-57469, V-57471, V-57473, V-57475, V-57477, V-57479. - The following were removed by DoD Consensus: V-1158, V-1159, V-3457, V-3458, V-14254, V-15719, V-26471, V-26491, V-26495, V-36772. **Windows 8 / 8.1 Benchmark, V1R17:** - V-14236 - Updated OVAL content in conjunction with modifications to the requirement in the manual STIG. - V-32274 - Updated OVAL with new certificate information. - Disabled the following rules in OVAL in conjunction with the removal of the requirements from the manual STIG: V-1158, V-1159, V-3457, V-3458, V-14254, V-15714, V-15715, V-15717, V-15719, V-26471, V-26491, V-26495, V-56511, V-57453, V-57455, V-57457, V-57463, V-57465, V-57467, V-57469, V-57471, V-57473, V-57475, V-57477, V-57479.	27 January 2017

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
V1R15	- Windows 8/ 8.1 STIG	- V-15505 - Updated for v5 of McAfee agent. - V-32272 - Updated PKE-related requirement with current certificates. - V-32273 - Updated PKE-related requirement with current certificates. - V-32274 - Updated PKE-related requirement with current certificates. - V-36663 - Removed BIOS-related requirement as outside of OS scope. - V-36664 - Removed BIOS-related requirement as outside of OS scope. - V-40195 - Removed BIOS-related requirement as outside of OS scope. - V-40237 - Updated PKE-related requirement with current certificates. - V-43243 - Updated for application name change to OneDrive. - V-57457 - Clarified requirement for location of Windows Error Reporting data. - V-57461 - Removed Windows Error Reporting port requirement; not security related. **Windows 8 / 8.1 Benchmark, V1R16:** - V-32272 - Updated OVAL to reference current certificates. - V-32273 - Updated OVAL to reference current certificates. - V-32274 - Updated OVAL to reference current certificates. - V-40237 - Updated OVAL to reference current certificates. - V-43239 - Added new OVAL content.	28 October 2016
V1R14	- Windows 8/ 8.1 STIG	- V-1107 - Clarified with regard to selection of 24 for password history. - V-36663 - Clarified with regard to virtual machines. - V-36664 - Clarified with regard to virtual machines. - V-40195 - Clarified with regard to virtual machines. - V-43239 - Changed back to enabled to aid incident response.	22 July 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-57637 - Changed to CAT II. Updated PowerShell query used to determine AppLocker effective policy. - Alternate CAT I requirements have been added to the STIG to replace EMET if it has not been installed. - V-68843 Alternate DEP configuration. - V-68847 Alternate SEHOP configuration. - Existing EMET requirements are NA if the alternate settings are configured. - V-39137, V-36701, V-36702, V-36703, V-36704, V-36705, V-36706. **Windows 8 / 8.1 Benchmark, V1R15:** - Added SCAP 1.2 Validation Fixes to Windows 8 STIG. - V-68843 - Added OVAL. - V-68847 - Added OVAL. - Existing EMET requirements are NA if the alternate settings are configured. - V-39137, V-36701, V-36702, V-36703, V-36704, V-36705, V-36706.	
V1R13	- Windows 8/ 8.1 STIG	- V-1080 - Removed requirement due to excessive event generation. - V-1088 - Removed requirement due to excessive event generation. - V-1131 - Removed requirement referencing Enpasflt password filter which is no longer supported. - V-1150 - Raised requirement for Windows built-in password complexity to a CAT II. - V-1155 - Removed references to Windows 8.0. Updated requirement to refer to the built-in "Local account" group. - V-15671 - Removed requirement preventing root certificate updates from Microsoft. - V-26486 - Removed references to Windows 8.0. Updated requirement to refer to the built-in "Local account" group. - V-26544 - Removed requirement due to excessive event generation.	22 April 2016

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- V-26545 - Removed requirement due to excessive event generation. - V-26579 - Corrected event log size policy name in Fix. - V-26580 - Increased Security event log size to 196608 KB or greater. Corrected event log size policy name in Fix. - V-26581 - Corrected event log size policy name in Fix. - V-26582 - Corrected event log size policy name in Fix. - V-36669 - Removed requirement due to excessive event generation. - V-36670 - Removed audit review policy requirement. - V-36671 - Removed audit archive policy requirement. - V-36672 - Removed audit archive policy requirement. - V-36702 - Updated for EMET 5.5. - V-36703 - Updated for EMET 5.5. - V-36704 - Updated for EMET 5.5. - V-36707 - Revised requirement to enable Windows SmartScreen filter, raised to a CAT II. - V-39137 - Updated for EMET 5.5. - V-45589 - Removed requirement to define a group for local administrator accounts. Addressed by the built-in "Local account" group. - Removed the following requirements, applicable to Windows 8.0, which is no longer supported: - V-36737, V-36741, V-36748, V-36751. - Updated the following requirements to remove references to specific versions of Windows 8: - V-15713, V-36710, V-43237, V-43238, V-43239, V-43240, V-43241, V-43242, V-43243, V-43244, V-43245, V-43303, V-43304, V-43305, V-43306, V-43307, V-43308, V-43310, V-43312, V-43313. **Windows 8/8.1 Benchmark, V1R14:** - V-1081 - Added OVAL.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1155 - Modified the OVAL to include a check for the Local account and Local account and member of Administrators which includes the NT Authority prefix. - V-1155 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-3347 - Added OVAL. - V-7002 - Added OVAL. - V-15671 - Disabled Rule. - V-26483 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26484 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26485 - Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26486 - Modified the OVAL to include a check for the Local account and Local account and member of Administrators which includes the NT Authority prefix. Modified the OVAL to include an equals check for the Enterprise Admins group. - V-26544 - Disabled Rule. - V-26545 - Disabled Rule. - V-26580 - Modified OVAL to change MaxSize value to 196608. - V-36702 - Updated for EMET 5.5. - V-36703 - Updated for EMET 5.5. - V-36704 - Updated for EMET 5.5. - V-36707 - Disabled Rule. - V-36710 - Modified the OVAL to match the updated STIG requirement. - V-39137 - Updated for EMET 5.5. - V-45589 - Disabled Rule.	
V1R12	- Windows 8/ 8.1 STIG	- Added Section 1.7 Product Approval Disclaimer to the STIG Overview document. - V-1073 - Updated to note the initial release of Windows 8 will not be supported after 12 Jan 2016. - V-1152 - Clarification that requirement is enforcing default permissions. - V-26070 - Clarification that requirement is enforcing default permissions.	22 January 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-32282 - Clarification that requirement is enforcing default permissions. - V-36690 - Removed requirement. - V-36691 - Removed requirement. - V-36756 - Removed requirement. **Windows 8/8.1 Benchmark, V1R13:** - V-1073 - Updated OVAL content to support Windows 8.1 systems or higher. - V-36690 - Disabled OVAL content. - V-36691 - Disabled OVAL content.	
V1R11	- Windows 8/ 8.1 STIG	- V-1074 - Removed Symantec from requirement. - V-1091 - Removed requirement. - V-14248 - Clarification on use for administration. Added notes on use of Restricted Admin mode. - V-14250 - Removed requirement. - V-26473 - Clarification on use for administration. Added notes on use of Restricted Admin mode. - V-43246 - Removed requirement. - V-57637 - Application Whitelisting requirement was raised to CAT I. - The following were updated to correct policy names as wells as miscellaneous text updates: V-1141, V-1158, V-1174, V-4116, V-4438, V-21956, V-21964. - The following were updated to change IAO references to ISSO as wells as miscellaneous text updates: V-1072, V-1081, V-1130, V-1157, V-1168, V-2908, V-3338, V-3339, V-3347, V-3470, V-4443, V-6840, V-14224, V-15823, V-36656, V-36658, V-36659, V-36708, V-36757. **Windows 8/8.1 Benchmark, V1R12:** - V-1091 Removed requirement. - V-15823 Matched file extensions case insensitivity. - V-40237 Updated to search an additional path when certificate is installed via group policy. - Removed unreferenced OVAL content.	23 October 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R10	- Windows 8/ 8.1 STIG	- Added Section 1.6 Other Considerations to the STIG Overview document. - V-1112 – Clarification. - V-1148 – Clarification. - V-3385 - Corrected policy name. - V-39137 - Updated to require EMET v5.x. Support for v4.x ended 09 June 2015. - V-57637 - Requirement added for whitelisting. - CCI referenced for the following changed to CCI-000366. - V-36741, V-36742, V-36743, V-36744, V-36745, V-36746, V-36747, V-36748, V-36749, V-36750, V-36751, V-43304, V-43305, V-43306, V-43307, V-43308, V-43310, V-43312, V-43313. **Windows 8/8.1 Benchmark, V1R11:** - V-1099 Modified check for account lockout policy. - V-3338 Modified check against registry value. - V-3339 Modified check against registry value. - V-3340 Modified check against registry value. - V-4443 Modified check against registry value. - V-32272 Added registry check. - V-32273 Added registry check. - V-32274 Added registry check. - V-39137 Updated check for EMET.	24 July 2015
V1R9	- Windows 8 STIG	- STIG Support Helpdesk email has been updated to disa.stig_spt@mail.mil. - DISA Field Security Operations (FSO) changed to DISA. - V-1090 - Requirement is NA for non-domain joined systems. - V-1127 - Typo corrected in Check/Fix - "domain member server" should be "domain workstation". - V-4108 - Update note regarding use of audit server. - V-15680 - Requirement is NA for domain joined systems. - V-15719 - Requirement is NA for non-domain joined systems.	24 April 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26579 - Requirement is NA if audit records are written directly to an audit server. - V-26580 - Requirement is NA if audit records are written directly to an audit server. - V-26581 - Requirement is NA if audit records are written directly to an audit server. - V-26582 - Requirement is NA if audit records are written directly to an audit server. - EMET - The following requirements are applicable to unclassified systems: - V-39137 - Requirement to have EMET installed changed to a CAT I. Note added regarding end of support for V4.x in June 2015. - V-36701, V-36702, V-36703, V-36704, V-36705, V-36706. **Windows 8 Benchmark, V1R10:** - V-1090 added applicability statement. - V-1098 added OVAL check for Lockout Threshold. - V-1099 added OVAL check for Lockout Threshold. - V-15680 applicability statement will be added; setting is NA for domain systems. - V-15715 added to benchmark. - V-15719 added applicability statement. - V-56511 added to benchmark. - V-57453 added to benchmark. - V-57455 added to benchmark. - V-57463 added to benchmark. - V-57465 added to benchmark. - V-57467 added to benchmark. - V-57469 added to benchmark. - V-57471 added to benchmark. - V-57473 added to benchmark. - V-57475 added to benchmark. - V-57477 added to benchmark. - V-57479 added to benchmark. - Added XCCDF profile to exclude intensive checks when used on systems with a large number of user accounts.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R8	- Windows 8 STIG	- Windows Error Reporting requirements have been updated/added to enable error reporting and maintain locally. STIG IDs have been updated to organize the requirements. - V-3471 - Error Reporting - Removed, replaced by V-15715. - V-15714 - Error Reporting - Logging - Updated Severity. - V-15715 - Error Reporting - Added to enable error reporting. - V-15717 - Error Reporting - Additional Data - Updated to enable. - V-56511 - Error Reporting - Service - Added - V-57453 - Error Reporting - Throttle Data – Added. - V-57455 - Error Reporting - Inhibit User Notifications – Added. - V-57457 - Error Reporting - Configure Reporting Server Name – Added. - V-57459 - Error Reporting - Configure Secure Sockets Layer (SSL) – Added. - V-57461 - Error Reporting - Configure Reporting Port Number – Added. - V-57463 - Error Reporting - Enable Report Archive – Added. - V-57465 - Error Reporting - Configure Report Archive – Added. - V-57467 - Error Reporting - Maximum Archived Reports – Added. - V-57469 - Error Reporting - Enable Error Queuing – Added. - V-57471 - Error Reporting - Queuing Behavior – Added. - V-57473 - Error Reporting - Maximum Queued Reports – Added. - V-57475 - Error Reporting - Queue Reporting Interval – Added. - V-57477 - Error Reporting - Configure Default Consent – Added. - V-57479 - Error Reporting - Configure Consent Overrides – Added.	23 January 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- The following requirements have been updated to account for changes in the group name to assign deny rights to local administrator accounts: - V-1155 - Deny Access from the Network. - V-26486 - Deny log on through Remote Desktop \ Terminal Services. - V-45589 - Define group for deny rights. - V-15712 - Search - Exchange Folder Indexing - Updated to allow for specific exception. - V-15713 - Microsoft Active Protection Service - Updated for policy name change in Windows 8.1. - V-36710 - Automatic download of updates from the Windows Store - Updated for policy name change in Windows 8.1. - V-43239 - Command line data for process creation events - Requirement reversed due to potential to save clear text passwords. - The following have been updated to include reference to Microsoft article providing update information for Windows 8 default apps. - V-36741 – Bing. - V-36742 – Finance. - V-36743 – Maps. - V-36744 – News. - V-36745 – Sports. - V-36746 – Travel. - V-36747 – Weather. - V-36748 – Camera. - V-36749 – Reader. - V-36750 - Communications (Mail, People, Messaging, Calendar). - V-36751 – Photos. - V-43304 – Alarms. - V-43305 – Calculator. - V-43306 - Food and Drink. - V-43307 - Health and Fitness. - V-43308 - Help + Tips. - V-43310 - Reading List. - V-43312 – Scan. - V-43313 - Sound Recorder.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-56421 - Input Panel Password Security – New. **Windows 8 Benchmark, V1R9:** - V-1089 - Added OVAL content for the "Legal Notice Display" requirement. - V-1155 - Revised OVAL content to allow for the "DeniedNetworkAccess" group. Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-15717 - Revised OVAL content to require the "Do not send additional data" setting to be disabled. - V-26359 - Added OVAL content for the "Legal Banner Dialog Box Title" requirement. - V-26470 - Added OVAL content for the "Access this computer from the network" user right requirement. - V-26471 - Added OVAL content for the "Adjust memory quotas for a process" user right requirement. - V-26472 - Added OVAL content for the "Allow log on locally" user right requirement. - V-26474 - Added OVAL content for the "Back up files and directories" user right requirement. - V-26475 - Added OVAL content for the "Bypass traverse checking" user right requirement. - V-26476 - Added OVAL content for the "Change the system time" user right requirement. - V-26477 - Added OVAL content for the "Change the time zone" user right requirement. - V-26478 - Added OVAL content for the "Create a pagefile" user right requirement. - V-26480 - Added OVAL content for the "Create global objects" user right requirement. - V-26482 - Added OVAL content for the "Create symbolic links" user right requirement.	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- V-26483 - Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26484 - Corrected the "Deny log on as a service" for non-domain systems to include no entries instead of the Guests group. Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26485 - Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26486 - Revised OVAL content to allow for the "DeniedNetworkAccess" group. Revised pattern match for the "Enterprise Admins" group to resolve false positives when assigning the group the user right and the domain prefix is present. - V-26488 - Added OVAL content for the "Force shutdown from a remote system" user right requirement. - V-26489 - Added OVAL content for the "Generate security audits" user right requirement. - V-26490 - Added OVAL content for the "Impersonate a client after authentication" user right requirement. - V-26491 - Added OVAL content for the "Increase a process working set" user right requirement. - V-26492 - Added OVAL content for the "Increase scheduling priority" user right requirement. - V-26493 - Added OVAL content for the "Load and unload device drivers" user right requirement. - V-26496 - Added OVAL content for the "Manage auditing and security log" user right requirement.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26498 - Added OVAL content for the "Modify firmware environment values" user right requirement. - V-26499 - Added OVAL content for the "Perform volume maintenance tasks" user right requirement. - V-26500 - Added OVAL content for the "Profile single process" user right requirement. - V-26501 - Added OVAL content for the "Profile system performance" user right requirement. - V-26502 - Added OVAL content for the "Remove computer from docking station" user right requirement. - V-26504 - Added OVAL content for the "Restore files and directories" user right requirement. - V-26505 - Added OVAL content for the "Shut down the system" user right requirement. - V-26506 - Added OVAL content for the "Take ownership of files or other objects" user right requirement. - V-32272 - Added OVAL content for the "DoD Root Certificate" requirement. - V-32273 - Added OVAL content for the "External CA Root Certificate" requirement. - V-32274 - Added OVAL content for the "DoD Interoperability Root CA 1 to DoD Root CA 2 cross-certificate" requirement. - V-40237 - Added OVAL content for the "US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate" requirement. - V-45589 - Revised OVAL content to allow for the "DeniedNetworkAccess" group and the KB2871997 update.	
V1R7	- Windows 8 STIG	- Control Correlation Identifiers (CCIs) added to requirements. - V-1127 Administrator Group Membership - Clarification of accounts allowed for AD admin platforms.	28 October 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- EMET requirements have been changed back to CAT II. EMET V4.1 Update 1 or later required. - V-39137 EMET must be installed on the system. - V-36701 EMET ASLR must be enabled. - V-36702 EMET default protections for IE must be enabled. - V-36703 EMET default protections for recommended software must be enabled. - V-36704 EMET default protections for popular software must be enabled. - V-36705 EMET Data Execution Prevention must be enabled. - V-36706 EMET SEHOP must be enabled. **Benchmark\Oval Updates:** - Oval for EMET updated based on requirement for EMET V4.1 Update 1. - V-39137 EMET must be installed on the system.	
V1R6	- Windows 8 STIG	- The following requirements have been removed as not affecting this version of Windows: - V-14255 Publish to Web. - V-14257 Windows Messenger Experience Improvement. - V-14258 Search Companion Content File Updates. - V-15673 Internet Connection Wizard ISP Downloads. - V-15675 Windows Registration Wizard. - V-36729 Simple TCP/IP Service - Updated Check to look for the service not a file. **Benchmark/Oval Updates:** - V-1090 - Added OVAL content for the requirement. - V-1099 - Removed alternate test put in place for older versions of Policy Auditor and SCAP Compliance Checker.	25 July 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1113 - Updated OVAL content to check for the SID instead of the account name. - V-1114 - Updated OVAL content to check for the SID instead of the account name. - V-1115 - Updated OVAL content to check for the SID instead of the account name. - V-1163 - Added test for V-6831 to the definition as an alternate method for closing the vulnerability. - V-1164 - Added test for V-6831 to the definition as an alternate method for closing the vulnerability. - V-3340 - Updated OVAL content to allow for “Not Configured” as an acceptable option to close the vulnerability. - V-14235 - Updated OVAL content to allow for more restrictive settings. - V-14236 - Updated OVAL content to allow for more restrictive settings. - V-15672 - Added OVAL content for the requirement. - V-15687 - Added OVAL content for the requirement. - V-15722 - Added OVAL content for the requirement. - V-15823 - Added OVAL content for the requirement. - V-16047 - Added OVAL content for the requirement. - V-26503 - Updated OVAL content to allow for no accounts to be assigned to the user right. - V-36676- Added OVAL content for the requirement. - V-36709 - Added OVAL content for the requirement.	
V1R5	- Windows 8 STIG	- Overview document updated to note inclusion of Windows 8.1. - V-1127 Administrators Group Membership - Added comment related to AD admin platforms. - V-1155 Deny access from the network - Updated to incorporate "DenyNetworkAccess" group defined in V-45589 or new built-in	25 April 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		accounts for Windows 8.1. Added comment related to AD admin platforms. - V-26472 Allow log on locally - Added comment related to AD admin platforms. - V-26486 Deny log on through Remote Desktop Services - Updated to incorporate "DenyNetworkAccess" group defined in V-45589 or new built-in accounts for Windows 8.1. Added comment related to AD admin platforms. - V-45589 - New - A group named DenyNetworkAccess must be defined on domain systems to include all local administrator accounts. - EMET requirements have been changed to CAT IV, pending further resolution. - V-39137 EMET must be installed on the system. - V-36701 EMET ASLR must be enabled. - V-36702 EMET default protections for IE must be enabled. - V-36703 EMET default protections for recommended software must be enabled. - V-36704 EMET default protections for popular software must be enabled. - V-36705 EMET Data Execution Prevention must be enabled. - V-36706 EMET SEHOP must be enabled. - The following default app requirements have been added or updated to reflect Windows 8.1 or to allow an alternate update method. - V-36737 Windows 8 default SkyDrive app. - V-36741 Windows 8 default Bing app. - V-36742 Windows 8 default Finance app. - V-36743 Windows 8 default Maps app. - V-36744 Windows 8 default News app. - V-36745 Windows 8 default Sports app. - V-36746 Windows 8 default Travel app. - V-36747 Windows 8 default Weather app. - V-36748 Windows 8 default Camera app. - V-36749 Windows 8 default Reader app.	

REVISION HISTORY			
Revision Number	Document Revised	Description of Change	Release Date
		- V-36750 Windows 8 default Communications apps. - V-36751 Windows 8 default Photos app. - V-43303 Windows 8 default Skype app. - V-43304 Windows 8 default Alarms app. - V-43305 Windows 8 default Calculator app. - V-43306 Windows 8 default Food and Drink app. - V-43307 Windows 8 default Health and Fitness app. - V-43308 Windows 8 default Help + Tips app. - V-43310 Windows 8 default Reading List app. - V-43312 Windows 8 default Scan app. - V-43313 Windows 8 default Sound Recorder app. - The following requirements have been added for Windows 8.1. - V-43237 Camera access from the lock screen must be disabled. - V-43238 The display of slide shows on the lock screen must be disabled. - V-43239 Command line data must be included in process creation events. - V-43240 The network selection user interface (UI) must not be displayed on the logon screen. - V-43241 The setting to allow Microsoft accounts to be optional for modern style apps must be enabled. - V-43242 Information shared with Bing in Search must be configured to the most restrictive setting. - V-43243 The use of SkyDrive for storage must be disabled. - V-43244 The option to update to the latest version of Windows from the Store must be turned off. - V-43245 Automatically signing in the last interactive user after a system-initiated restart must be disabled. - V-43246 Windows Update must not connect to any Internet locations.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Benchmark/Oval Updates: - V-1145 Updated content to verify no passwords are stored in the “DefaultPassword” registry value. - V-1155 Added automated content for the vulnerability. - V-26846 Added automated content for the vulnerability. - V-36703 Updated content to use variable checks in lieu of multiple tests. - V-36704 Updated content to use variable checks in lieu of multiple tests. - V-36705 Updated content to allow for “Always On” for Data Execution Prevention. - V-45589 Added automated content for the vulnerability.	
V1R4	- Windows 8 STIG	- V-36723 Security Event Log Permissions - Corrected Fix section to reference "Security". - V-26575 6to4 State - Updated policy name in Fix section to include "Set". - V-26576 IP-HTTPS State - Updated policy name in Fix section to include "Set". - V-26577 ISATAP State - Updated policy name in Fix section to include "Set". - V-26578 Teredo State - Updated policy name in Fix section to include "Set". - BIOS requirements updated. - V-36663 Admin password - User-level access moved to separate requirement (V-40195). - V-36664 Removable Media - Updated for clarification. - V-40195 User-level access - Separated from V-36663. - PKE requirements updated to define applicable network. - V-32272 DoD Root Certificate. - V-32273 External CA Root Certificate. - V-32274 DoD Interoperability Root CA 1 to DoD Root CA 2 cross certificate - Check updated with new thumbprint. - V-40237 DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate.	24 January 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Windows Firewall requirements have been moved from Windows STIGs to a separate Windows Firewall STIG. - Added V-42420 General firewall requirement for Windows. - Removed V-17415 through V-17449. **Benchmark/Oval Updates:** - Added OVAL content for user right vulnerabilities: - V-26483 Deny log on as a batch job. - V-26484 Deny log on as a service. - V-26485 Deny log on locally. - Added OVAL content for EMET vulnerabilities: - V-36701 EMET Address Space Layout Randomization (ASLR). - V-36702 EMET Default Protections for Internet Explorer. - V-36703 EMET Default Protections for Recommended Software. - V-36704 EMET Default Protections for Popular Software. - V-36705 EMET Data Execution Prevention (DEP). - V-36706 EMET Structured Exception Handler Overwrite Protection (SEHOP). - V-39137 EMET Installation.	
V1R3	- Windows 8 STIG	- The following section was removed from the Overview document. IAVMs are no longer included with Windows STIGs. 4.2 IAVM Checks - V-3480 Media Player Disable Automatic Updates - typo correction in Vulnerability Discussion. - V-14228 Audit Access of Global System Objects - policy name correction. - V-17420 Windows Firewall Domain Display Notifications - policy name correction. - V-17430 Windows Firewall Private Display Notifications - policy selection text update.	25 October 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-17440 Windows Firewall Public Display Notifications - policy selection text update. - V-32274 DoD Interop Root CA 1 to DoD Root CA 2 cross cert - updated with new certificate information from PKE. - V-36684 User Enumeration on domain-joined computers - policy name correction. - V-36701 EMET System ASLR - updated to include V4.0 policy name change. - V-36705 EMET System DEP - updated to include V4.0 policy name change. - V-36706 EMET System SEHOP - updated to include V4.0 policy name change. - V-40237 US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate - new cross cert requirement from PKE.	
V1R2	- Windows 8 STIG	- Section on the Enhanced Mitigation Experience Toolkit (EMET) moved to Section 5 of the Overview document. - V-1080 File Auditing Configuration - added Global Object Access Auditing as a configuration option. - V-1088 Registry Key Auditing - added Global Object Access Auditing as a configuration option. Replaced V-36725 and V-36726. - V-4448 Group Policy - Registry Policy Processing - corrected policy name in Fix. - V-26475 Bypass traverse checking - updated to allow Window Manager\Window Manager Group. - V-26485 Deny log on locally - clarification added for workstations dedicated to management of Active Directory. - V-26491 Increase a process working set - updated to allow Window Manager\Window Manager Group. - V-36660 Browsers and email with administrator accounts - updated for clarification. - V-36722 Permissions for the Application event log must prevent access by non-privileged	26 July 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		accounts - updated to correct default permissions. - V-36724 Permissions for the System event log must prevent access by non-privileged accounts - updated to correct default permissions. - V-36727 Hyper-V must not be installed on a workstation - updated for clarification. - V-36770 Local Administrators privileged token filtered - updated for clarification. - Requirements for Enhanced Mitigation Experience Toolkit (EMET) added or updated. - V-39137 EMET must be installed on the system. - new requirement. - V-36703 EMET Default Protections for Recommended Software must be enabled. - updated for EMET 4.0. - V-36704 EMET Default Protections for Popular Software must be enabled. - updated for EMET 4.0. - V-36705 EMET system-wide Data Execution Prevention (DEP) must be enabled and configured. - updated to require Application Opt Out. - V-36706 EMET system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be enabled and configured. - updated to require Application Opt Out.	