WINDOWS 7 STIG
REVISION HISTORY

Version 1, Release 29

26 January 2018

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R29	- Windows 7 STIG	- V-26470 - Updated to note allowed exception to access computer from the network user right. **Windows 7 Benchmark, V1R35:** - V-3347 - Modified to verify the status of the IIS features using wmi57 tests in lieu of registry tests. - V-68843 - Updated to ensure Windows 7 check content is separate from Windows 10. - V-68847 - Updated to ensure Windows 7 check content is separate from Windows 10.	26 January 2018
V1R28	- Windows 7 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 - Updated Fix to use custom administrative template for configuration. - V-73523 - Modified Check for DependOnService to only be a finding if SMBv1 is found. Updated Fix to use custom administrative template for configuration. - 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 7 Benchmark, V1R34:** - Removed OVAL content for the following as requirement has been removed from the STIG:	27 October 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-26475, V-26477, V-26502, V-26505, V-28285. - V-32282 - Added OVAL content to the benchmark. - V-73523 - Updated the OVAL content for SMBv1 Client requirement to be a finding only if SMBv1 is found.	
V1R27	- Windows 7 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-36439 - Updated Fix to use custom admin template instead of direct registry update. **Windows 7 Benchmark, V1R33:** - 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
V1R26	- Windows 7 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-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-73519 - Added requirement to disable Server Message Block (SMB) v1 on the SMB server.	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-73523 - Added requirement to disable Server Message Block (SMB) v1 on the SMB client. **Windows 7 Benchmark, V1R32:** - V-15505 - Added OVAL to check if one of the supported versions of the McAfee agents is installed and running. - V-73519 - Added OVAL to check if the SMBv1 protocol for the SMB server is disabled. - V-73523 - Added OVAL to check if the SMBv1 protocol for the SMB client is disabled. - Added new XCCDF profile to disable EMET checks where they are not applicable.	
V1R25	- Windows 7 STIG	- V-14236 - Changed User Account Control standard user elevation to automatically deny. - V-32274 - Updated expired certificate with replacement. - V-36757 - Added requirement to turn off Bluetooth unless organization approved. - V-36759 - Added requirement to turn off Bluetooth when not in use. - V-36762 - Added requirement to send notifications when Bluetooth devices attempt to connect. - V-72573 - Added requirement to turn off wireless interfaces when connected to a wired network. - V-72753 - Added requirement to disable WDigest. - Removed requirement to disable IPv6- V-14262. - Removed Error Reporting requirements: V-15714, V-15715, V-15717, V-56511, 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.	27 January 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Windows 7 Benchmark, V1R31: - 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-14262, V-15714, V-15715, V-15717, V-15719, V-26471, V-26491, V-26495, V-56511, V-57455, V-57457, V-57459, V-57463, V-57465, V-57467, V-57469, V-57471, V-57473, V-57475, V-57477, V-57479.	
V1R24	- Windows 7 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-57457 - Clarified requirement for location of Windows Error Reporting data. - V-57461 - Removed Windows Error Reporting port requirement; not security related. **Windows 7 Benchmark, V1R30:** - V-32272 - Updated OVAL to reference current certificates. - V-32273 - Updated OVAL to reference current certificates.	28 October 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-32274 - Updated OVAL to reference current certificates. - V-40237 - Updated OVAL to reference current certificates.	
V1R23	- Windows 7 STIG	- V-1107 - Clarified with regard to selection of 24 for password history. - V-1155 - Updated to require use of "Local account" to deny access on workstations. - V-26486 - Updated to require use of "Local account" to deny access on workstations. - 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-45589 - Removed requirement to define a group for local administrator accounts. - 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 7 Benchmark, V1R29:** - V-1155 - Modified OVAL content to remove DenyNetworkAccess/DeniedNetworkAccess groups. - V-26486 - Modified OVAL content to remove DenyNetworkAccess/DeniedNetworkAccess groups. - V-45589 - Disabled rule in OVAL. - V-68843 - Added OVAL. - V-68847 - Added OVAL.	22 July 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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.	
V1R22	- Windows 7 STIG	- Added Section 1.7 Product Approval Disclaimer to the STIG Overview document. - 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-1152 - Clarified requirement to maintain the default permissions. - V-15671 - Removed requirement preventing root certificate updates from Microsoft. - V-26070 - Clarified requirement to maintain the default permissions. - V-26544 - Removed requirement due to excessive event generation. - V-26545 - Removed requirement due to excessive event generation. - V-26580 - Increased Security event log size to 196608 KB or greater. - V-32282 - Clarified requirement to maintain the default permissions. - V-36669 - Removed requirement due to excessive event generation. - V-36702 - Updated for EMET 5.5. - V-36703 - Updated for EMET 5.5. - V-36704 - Updated for EMET 5.5. - V-39137 - Updated for EMET 5.5. **Windows 7 Benchmark, V1R28:** - V-1081 - Added OVAL. - 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.	22 April 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1155 - Modified the OVAL to include an equals check for the Enterprise Admins group. - 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 accept the Everyone group as a passing state. 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-39137 - Updated for EMET 5.5.	
V1R21	- Windows 7 STIG	- V-1074 - Removed Symantec from requirement. - V-1077 - Updated to allow default permissions. - V-1091 - Removed requirement. - V-1137 - 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-26496 - Updated "Manage auditing and security log" user right to allow "Administrators".	23 October 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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-21964. - The following were updated to change IAO references to ISSO as wells as miscellaneous text updates. In some cases Documentable tags may have been removed and replaced with requirements for documentation. V-1072, V-1081, V-1093, V-1122, V-1127, V-1130, V-1140, V-1151, V-1153, V-1157, V-1168, V-2908, V-3245, V-3347, V-3382, V-3470, V-3666, V-6840, V-14224, V-14225, V-14262, V-15823, V-28285. **Windows 7 Benchmark, V1R27:** - V-1091 Removed requirement. - V-4443 Updated the OVAL to match the path described in the STIG System\CurrentControlSet\Services\Sysmonlog. - V-15823 Matched file extensions case insensitivity. - V-26496 Updated "Manage auditing and security log" user right: Allow "Administrators". - V-40237 Updated to search an additional path when certificate is installed via group policy. - Removed unreferenced OVAL content.	
V1R20	- Windows 7 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. - The following have been updated to add Fix details as well as miscellaneous text updates.	24 July 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-1077, V-1089, V-1097, V-1098, V-1099, V-1102, V-1104, V-1105, V-1107, V-1113, V-1114, V-1115, V-1135, V-1152, V-2372, V-3337, V-3338, V-3339, V-3380, V-4443, V-14231, V-16006, V-16047, V-18010, V-21950, V-21951, V-21952, V-21953, V-21954, V-21955, V-21956, V-26469, V-26470, V-26471, V-26473, V-26474, V-26475, V-26476, V-26477, V-26478, V-26479, V-26480, V-26481, V-26482, V-26487, V-26488, V-26489, V-26490, V-26491, V-26492, V-26493, V-26494, V-26495, V-26496, V-26497, V-26498, V-26499, V-26500, V-26501, V-26502, V-26503, V-26504, V-26505, V-26506. **Windows 7 Benchmark, V1R26:** - V-1099 Modified check for account lockout policy. - V-3338 Modified check against registry value. - V-3340 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.	
V1R19	- Windows 7 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 - Changed from Documentable to NA if audit records are written directly to an audit server. - V-15680 - Requirement is NA for domain joined systems. - V-15719 - Requirement is NA for non-domain joined systems. - V-26579 - Requirement is NA if audit records are written directly to an audit server.	24 April 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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 7 Benchmark, V1R25:** - 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-15719 added applicability statement. - V-15823 OVAL updated to improve efficiency. - V-56511 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.	
V1R18	- Windows 7 STIG	- Windows Error Reporting requirements have been updated/added to enable error reporting	23 January 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		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 - Updated to enable error reporting. - V-15717 - Error Reporting - Additional Data - Updated to enable. - V-56511 - Error Reporting - Service – 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. - 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26486 - Deny log on through Remote Desktop \ Terminal Services. - V-45589 - Define group for deny rights. - The following have been updated to allow for specific exceptions: - V-15724 - Gadgets - Unsigned Gadgets. - V-15725 - Gadgets - More Gadgets Link. - V-15726 - Gadgets - User Installed Gadgets. - V-15712 - Search - Exchange Folder Indexing. - V-14262 - IPv6 Transition - Updated with additional registry value. - V-15682 - RSS Attachment Downloads - Updated for policy name change (depending on IE version). - V-17900 - Disallow AutoPlay/Autorun from Autorun.inf - Removed, replaced by V-22692. - V-22692 - Default Autorun Behavior - Updated to Cat I, consistent with the rest of Windows STIGS. - V-40237 - US DoD CCEB Interoperability Root CA 1 to DoD Root CA 2 cross-certificate - Corrected STIG ID. - V-56421 - Input Panel Password Security – New. **Windows 7 Benchmark, V1R24:** - V-1113 - Revised pattern match for the Built-in Guest account SID to resolve false positives. - V-1114 - Revised pattern match for the Built-in Guest account SID to resolve false positives. - V-1115 - Revised pattern match for the Built-in Admin account SID to resolve false positives. - V-1155 - Revised OVAL content to allow for the "DeniedNetworkAccess" group, the "Local account" group and the "Local account and member of Administrators group" 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-14262 - Revised OVAL content to allow for an alternate value. - V-15715 - Revised OVAL content to require the "Disable Windows Error Reporting" setting to be disabled. - V-15717 - Revised OVAL content to require the "Do not send additional data" setting to be disabled. - V-15724 - Revised OVAL definition to allow the requirement to be closed if Windows Gadgets are disabled. - 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 - 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, the "Local account" group and the "Local account and member of Administrators group" 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-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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-45589 - Revised OVAL content to allow for the "DeniedNetworkAccess" group and the KB2871997 update.	
V1R17	- Windows 7 STIG	- Control Correlation Identifiers (CCIs) added to requirements. - V-1127 Administrator Group Membership - Clarification of accounts allowed for AD admin platforms. - 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. - V-36703 EMET default protections for recommended software must be enabled. - V-36704 EMET default protections for popular software must be enabled.	28 October 2014
V1R16	- Windows 7 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.	25 July 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-15673 Internet Connection Wizard ISP Downloads. - V-15675 Windows Registration Wizard. - V-3455 Remote Desktop Temp Folders - Typo correction in Vulnerability Discussion. - V-6836 Minimum Password Length - Fix detail added, correcting typo. - V-14271 Application Account Passwords - Typo correction in Vulnerability Discussion. Removed Active Directory references from Check. **Benchmark/Oval Updates:** - V-1099 - Removed alternate test put in place for older versions of Policy Auditor and SCAP Compliance Checker. - 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-14235 - Updated OVAL content to allow for more restrictive settings. - V-14236 - Updated OVAL content to allow for more restrictive settings. - V-26489 - Updated OVAL content to allow for no accounts to be assigned to the user right. - V-26501 - Modified content to resolve case-sensitivity issue with NT SERVICE\WdiServiceHost. - V-26503 - Updated OVAL content to allow for no accounts to be assigned to the user right. - V-34974 - Added OVAL content for the requirement.	
V1R15	- Windows 7 STIG	- 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. Added comment related to AD admin platforms.	25 April 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. 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. **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-26475 Updated content to verify the Users group is assigned the user right in lieu of the Authenticated Users group. - 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-36705 Updated content to allow for "Always On" for Data Execution Prevention. - V-39137 Updated content to verify EMET version using the registry in lieu of the version of the EMET DLL file. - V-45589 Added automated content for the vulnerability.	
V1R14	- Windows 7 STIG	- BIOS requirements added to STIG: - V-36663 Admin password. - V-36664 Removable Media, CAT I. - V-40195 User-level access. - 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. - Windows Firewall requirements have been moved from Windows STIGs to a separate Windows Firewall STIG. - V-42420 General firewall requirement for Windows – Added. - V-17415 through V-17449 – Removed. **Benchmark/Oval Updates:** - V-1113 Disable Guest Account – Updated OVAL content to check for the SID instead of the account name. - V-1114 Rename Built-in Guest Account – Updated OVAL content to check for the SID instead of the account name. - V-1115 Rename Built-in Administrator – Updated OVAL content to check for the SID instead of the account name. - V-3472 Windows Time Service – Removed OVAL content due to inability to verify possible NTP servers as a secure, authorized time source.	24 January 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-15823 Software Certificate Installation Files – Added OVAL content. - V-16047 Built-in Admin Account Status – Updated OVAL content to check for the SID instead of the account name. - Added OVAL content for several user right vulnerabilities: - V-26470 Access this computer from the network. - V-26471 Adjust memory quotas for a process. - V-26472 Allow log on locally. - V-26474 Back up files and directories. - V-26475 Bypass traverse checking. - V-26476 Change the system time. - V-26477 Change the time zone. - V-26478 Create a pagefile. - V-26480 Create global objects. - V-26482 Create symbolic links. - V-26488 Force shutdown from a remote system. - V-26490 Impersonate a client after authentication. - V-26491 Increase a process working set. - V-26492 Increase scheduling priority. - V-26493 Load and unload device drivers. - V-26498 Modify firmware environment variables. - V-26499 Perform volume maintenance tasks. - V-26500 Profile single process. - V-26501 Profile system performance. - V-26502 Remove computer from docking station. - V-26504 Restore files and directories. - V-26505 Shut down the system. - V-26506 Take ownership of files or other objects.	
V1R13	- Windows 7 STIG	- The following sections were removed from the Overview document. Deviations or exceptions must follow standard adjudication process. IAVMs are no longer included with Windows STIGs. 2.1 ACL Deviations.	25 October 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		2.2 Application Exceptions. 2.3 IAVM Checks. - V-3480 Media Player Disable Automatic Updates - typo correction in Vulnerability Discussion. - V-3469 Group Policy Background Refresh - added requirement, consistent with other Windows STIGs. - V-16007 8dot3 Name Creation - removed from STIGs. - 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. - 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-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. - Readme.txt file - removed references to FOUO version of STIG no longer produced. **Benchmark/Oval Updates:** - V-14250 Configure Automatic Updates - removed from benchmark. A valid DoD WSUS cannot be verified via OVAL. - V-16007 8dot3 Name Creation - removed from benchmark. - V-36701 EMET ASLR Configuration - content added for the requirement.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-36702 EMET Default Protections for IE - content added for the requirement. - V-36703 EMET Default Protections for Recommended Software - content added for the requirement. - V-36704 EMET Default Protections for Popular Software - content added for the requirement. - V-36705 EMET System-wide DEP Configuration - content added for the requirement. - V-36706 EMET System-wide SEHOP Configuration - content added for the requirement. - V-39137 EMET must be installed - content added for the requirement.	
V1R12	- Windows 7 STIG	- Section on the Enhanced Mitigation Experience Toolkit (EMET) added to the Overview document. - V-1073 Supported Service Packs - updated for SP1 requirement. - 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. - V-1145 Disable Automatic Logon - updated to Cat II with Cat I severity override. - V-14231 Hide Computer - added registry value to check. - V-14250 Configure Automatic Updates - corrected registry path for location of WSUS server. - V-26485 Deny log on locally - clarification added for workstations dedicated to management of Active Directory. - V-36669 The system must be configured to audit Object Access - Handle Manipulation failures - added requirement. - Requirements added for Enhanced Mitigation Experience Toolkit (EMET).	26 July 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-39137 EMET must be installed on the system. - V-36701 EMET system-wide Address Space Layout Randomization (ASLR) must be enabled and configured. - V-36702 EMET Default Protections for Internet Explorer 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 system-wide Data Execution Prevention (DEP) must be enabled and configured. - V-36706 EMET system-wide Structured Exception Handler Overwrite Protection (SEHOP) must be enabled and configured. **Benchmark/Oval Updates:** - V-1073 Supported Service Packs - updated for SP1 requirement. - V-3340 Anonymous Access to Network Shares - updated to allow blank registry value or no registry value at all.	
V1R11	- Windows 7 STIG	- IAVMs are no longer incorporated in an FOUO version of the Windows STIGs. They will be produced as IAVM STIGs for the specific Windows versions. - V-34974 Always Install with Elevated Privileges Disabled - new Cat I requirement. **Pass the Hash/Credential Theft Mitigations** - Requirements have been added or updated to mitigate Pass the Hash/Credential Theft attacks in domains. - A section on this with a reference to a Microsoft document has been added to the STIG Overview document. - V-1127 Restricted Administrator Group Membership - changed to a Cat I, added requirement for domain workstation administrator group on domain systems.	29 March 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1140 Users with Administrative Privilege - changed to Cat I. - V-36451 Accounts with administrative privileges internet access - new Cat I. - V-36439 Built-in admin accounts filtered token enabled - new Cat II. - Several User Rights have been updated, restricting Domain and Enterprise Admins groups and/or local administrator accounts on domain systems. - V-1155 Deny Access from the Network. - V-26483 Deny log on as a batch job. - V-26484 Deny log on as a service. - V-26485 Deny log on locally. - V-26486 Deny log on through Remote Desktop Services. - Windows Firewall requirements notes have been updated to ensure comparable third party firewall settings are configured. - V-17415 Windows Firewall Domain - Enable Firewall. - V-17416 Windows Firewall Private - Enable Firewall. - V-17417 Windows Firewall Public - Enable Firewall. - V-17418 Windows Firewall Domain – Inbound. - V-17419 Windows Firewall Domain – Outbound. - V-17420 Windows Firewall Domain - Display Notifications. - V-17421 Windows Firewall Domain - Unicast Response. - V-17422 Windows Firewall Domain - Local Firewall Rules. - V-17423 Windows Firewall Domain - Local Connection Rules. - V-17424 Windows Firewall Domain - Log File. - V-17425 Windows Firewall Domain - Log Size.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-17426 Windows Firewall Domain - Log Dropped Packets. - V-17427 Windows Firewall Domain - Log Successful Connections. - V-17428 Windows Firewall Private – Inbound. - V-17429 Windows Firewall Private – Outbound. - V-17430 Windows Firewall Private - Display Notifications. - V-17431 Windows Firewall Private - Unicast Response. - V-17432 Windows Firewall Private - Local Firewall Rules. - V-17433 Windows Firewall Private - Local Connection Rules. - V-17434 Windows Firewall Private - Log File. - V-17435 Windows Firewall Private - Log Size. - V-17436 Windows Firewall Private - Log Dropped Packets. - V-17437 Windows Firewall Private - Log Successful Connections. - V-17438 Windows Firewall Public – Inbound. - V-17439 Windows Firewall Public – Outbound. - V-17440 Windows Firewall Public - Display Notifications. - V-17441 Windows Firewall Public - Unicast Response. - V-17442 Windows Firewall Public - Local Firewall Rules. - V-17443 Windows Firewall Public - Local Connection Rules. - V-17444 Windows Firewall Public - Log File. - V-17445 Windows Firewall Public - Log Size. - V-17446 Windows Firewall Public - Log Dropped Packets. - V-17447 Windows Firewall Public - Log Successful Connections.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-17448 Windows Firewall - IPv6 Block Protocols 41. - V-17449 Windows Firewall - IPv6 Block UDP 3544. - V-36440 Inbound Firewall Exception for Administration - new Cat II. **Benchmark/Oval Updates:** - The following were added. - V-1089 Legal Notice. - V-26359 Legal Banner Dialog Box Title. - The following were removed. - V-1155 User Right - Deny access from the network. - V-26484 User Right - Deny log on as a service. - V-26485 User Right - Deny log on locally.	
V1R10	- Windows 7 STIG	- V-1089 Legal Banner – corrected double dash in banner text. - V-14224 Backup Admin Account – updated to clarify. - V-32272 DoD Root Certificate – add reference for PKE Tools to Fix section. - V-32273 ECA Root Certificate – add reference for PKE Tools to Fix section. - V-32274 DoD Interoperability Root CA to DoD Root CA 2 cross cert – add reference for PKE Tools to Fix section. - Various editing corrections. **Benchmark\Oval Updates:** - V-26579 Maximum Log Size – Application – corrected to test for greater than or equals instead of equals. - V-26580 Maximum Log Size - Security – corrected to test for greater than or equals instead of equals. - V-26581 Maximum Log Size - Setup – corrected to test for greater than or equals instead of equals.	26 October 2012

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26582 Maximum Log Size - System – corrected to test for greater than or equals instead of equals. - V-26483 Deny log on as a batch job – removed, issue with tools being able to evaluate.	
V1R9	- Windows 7 STIG	- Overview Section 1.6 – updated email address for FSO STIG Customer Support. - New Cat I Requirement. - V-32282 Active Setup Registry Permissions. - 3 new PKE requirements added: - V-32272 DoD Root Certificate. - V-32273 ECA Root Certificate. - V-32274 DoD Interoperability Root CA to DoD Root CA 2 cross cert. - V-1073 Approved Service Packs – added note, support for initial release ends April 2013. - V-26359 Legal Banner Dialog Box Title – updated for consistency and clarification. Two predefined titles, clarification on site defined titles. - Various editing corrections.	27 July 2012
V1R8	- Windows 7 STIG	- V-1089 Legal Notice – corrected registry type referenced to reg_sz.	27 April 2012
V1R7	- Windows 7 STIG	- Various references to the Gold Disk removed. - V-3373 Maximum Machine Account Password Age – updated for clarification, 0 is not a valid option. - V-3457 TS/RDS Time Limit for Discontinued Session – updated for clarification, changed from 1 or less to equals 1. - V-3458 TS/RDS Time Limit for Idle Session – updated for clarification, 0 is not a valid option. - V-3471 Error Reporting – corrected policy path in Documentable section. - V-3472 Windows Time Service NTP – updated for clarification. - V-4438 TCP Data Retransmissions – corrected registry path, removed duplicate “system”.	27 January 2012

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-14249 TS/RDS Drive Redirection – corrected policy path. - V-14250 Configure Automatic Updates – updated for clarification, changed from Documentable to not a finding when pointing to a DoD WSUS server. - V-26475 Bypass Traverse Checking – corrected to “Users” vs. “Authenticated Users”.	
V1R6	- Windows 7 STIG	- V-1077 Event Log ACLs – added clarification to Fix on configuration of Eventlog account. - V-26576 IP-HTTPS State – Correct Policy name to "IP-HTTPS State".	28 October 2011
V1R5	- Windows 7 STIG	- Section 1.1 – corrected Windows 7 Business to Windows 7 Professional. - NEW CAT I requirement –V-26479 Create a token object (see below). - V-1073 Service Packs – updated to change focus to Cat I unsupported service packs vs. Cat II required service packs. - V-15505 HBSS McAfee Agent – updates to reflect current requirements. - Platinum only requirements changed to “Both”, Gold and Platinum. - V-1091, V-3382, V-3383, V-3666, V-6832, V-6833. - V-3382, V-3666 Corrected registry path referenced to “CurrentControlSet\Control”. - Several combined requirements have been separated to individual vulnerabilities in VMS to support SCAP automation. The original and new Vul IDs are listed below. See the STIG document for requirement details. - V-1089 Legal Notice separated the following: - V-26359 Legal Banner Title. - V-1093 Restrict Anonymous Network Shares separated the following: - V-26283 Restrict Anonymous SAM Enumeration. - V-1103 User Rights has been replaced by the following:	29 July 2011

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Note that V-26479 Create a token object is a Cat I. - V-26469 Access Credential Manager as a trusted caller. - V-26470 Access this computer from the network. - V-26471 Adjust memory quotas for a process. - V-26472 Allow log on locally. - V-26473 Allow log on through Remote Desktop Services. - V-26474 Back up files and directories. - V-26475 Bypass traverse checking. - V-26476 Change the system time. - V-26477 Change the time zone. - V-26478 Create a pagefile. - V-26479 Create a token object. - V-26480 Create global objects. - V-26481 Create permanent shared objects. - V-26482 Create symbolic links. - V-26483 Deny log on as a batch job. - V-26484 Deny log on as a service. - V-26485 Deny log on locally. - V-26486 Deny log on through Remote Desktop Services. - V-26487 Enable accounts to be trusted for delegation. - V-26488 Force shutdown from a remote system. - V-26489 Generate security audits. - V-26490 Impersonate a client after authentication. - V-26491 Increase a process working set. - V-26492 Increase scheduling priority. - V-26493 Load and unload device drivers. - V-26494 Lock pages in memory. - V-26495 Log on as a batch job. - V-28285 Log on as a service. - V-26496 Manage auditing and security log. - V-26497 Modify an object label. - V-26498 Modify firmware environment values. - V-26499 Perform volume maintenance tasks.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26500 Profile single process. - V-26501 Profile system performance. - V-26502 Remove computer from docking station. - V-26503 Replace a process level token. - V-26504 Restore files and directories. - V-26505 Shut down the system. - V-26506 Take ownership of files or other objects. - V-1102, V-1155 and V-18010 – STIG IDs have been updated to align with individual requirements from V-1103. - V-1118 Event Log Sizes has been replaced by the following: - V-26579 Maximum Log Size – Application. - V-26580 Maximum Log Size – Security. - V-26581 Maximum Log Size – Setup. - V-26582 Maximum Log Size – System. - V-6850 Audit Configuration has been replaced by the following: - V-26529 Audit - Credential Validation – Success. - V-26530 Audit - Credential Validation - Failure. - V-26531 Audit - Computer Account Management – Success. - V-26532 Audit - Computer Account Management – Failure. - V-26533 Audit - Other Account Management Events – Success. - V-26534 Audit - Other Account Management Events – Failure. - V-26535 Audit - Security Group Management – Success. - V-26536 Audit - Security Group Management – Failure. - V-26537 Audit - User Account Management – Success. - V-26538 Audit - User Account Management – Failure. - V-26539 Audit - Process Creation – Success. - V-26540 Audit - Logoff – Success.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26541 Audit - Logon – Success. - V-26542 Audit - Logon – Failure. - V-26543 Audit - Special Logon – Success. - V-26544 Audit - File System – Failure. - V-26545 Audit - Registry – Failure. - V-26546 Audit - Audit Policy Change – Success. - V-26547 Audit - Audit Policy Change – Failure. - V-26548 Audit - Authentication Policy Change – Success. - V-26549 Audit - Sensitive Privilege Use – Success. - V-26550 Audit - Sensitive Privilege Use – Failure. - V-26551 Audit - IPsec Driver – Success. - V-26552 Audit - IPsec Driver – Failure. - V-26553 Audit - Security State Change – Success. - V-26554 Audit - Security State Change – Failure. - V-26555 Audit - Security System Extension – Success. - V-26556 Audit - Security System Extension – Failure. - V-26557 Audit - System Integrity – Success. - V-26558 Audit - System Integrity – Failure. - V-14262 IPv6 Transition separated the following: - V-26575 6to4 State. - V-26576 IP-HTTPS State. - V-26577 ISATAP State. - V-26578 Teredo State.	
V1R4	- Windows 7 STIG	- NEW CAT I Requirement. - V-26070 Winlogon registry permissions. - V-14262 IPv6 - Correction to 0xffffffff to disable all interfaces due to discrepancies in supporting documentation. - The following requirements were updated to add registry information to the Checks and/or policy information to the Fixes. Additional	29 April 2011

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		updates noted where applicable. (The requirements themselves have not changed.) - V-1075, V-1084, V-1093, V-1153, V-1158, V-1159, V-1173, V-3338, V-3339, V-3340, V-3376, V-3377, V-3378, V-3379, V-3381, V-3382, V-3383, V-3385, V-3666, V-4108, V-4438, V-4442, V-4443, V-6834, V-14234, V-14235, V-14236, V-14237, V-14239, V-14240, V-14241, V-14242, V-16008. - Various – References to unsupported OS versions, the Windows Addendum and specific organizations removed. Spelling corrections with no impact to requirements. - Overview Document – Removed section on Gold / Platinum policies. Platinum only requirements will be changed to both with next release. Added section on IAVM checking.	
V1R3	- Windows 7 STIG	- Removed the following from Windows 7: - V-14267 Power Management - Require Password on Resume. - V-15669 Prohibit Internet Connection Sharing. - V-15716 Error Reporting – Error Notification. - V-21977 RSS – Basic feed authentication over HTTP. - V-14250 Configure Automatic Updates – removed statement from Check referencing incorrect registry value. - V-21954 Encryption Types for Kerberos – corrected Fix section, added “Future encryption types”. - V-21967 MSDT Interactive Communication – corrected registry value in Check section to “0”. - V-21978 Windows Anytime Upgrade – corrected registry path in Check section to HKLM\Software\Microsoft\Windows\Current Version\Policies\Explorer\WAU\. - The following requirements were updated to add registry information to the Checks and/or policy information to the Fixes. Additional	28 January 2011

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		updates noted where applicable. (The requirements themselves have not changed.).. - V-1085, V-1090, V-1091, V-1136, V-1141, V-1145, V-1151, V-1154, V-1157, V-1162, V-1163, V-1164, V-1165, V-1166, V-1171, V-1172, V-1174, V-3344, V-3373, V-3374, V-3375, V-3479 (corrected policy name to match current Security Options), V-4110, V-4111, V-4112 (corrected "IRDP" in Check), V-4113 (corrected policy name to match current Security Options), V-4116, V-6831, V-6832, V-6833, V-11806, V-14228, V-14229, V-14230, V-14231, V-14232, V-16007, V-17373 (corrected Fix to CDROM vs. Floppy).	
V1R2	- Windows 7 STIG	- V-1089 Legal Notice is not configured – removed False Positive note from VMS. Banner must be configured exactly as stated. Removed "," (comma) after COMSEC. Corresponding update made in "Analyze_only" security template. - V-1131 Strong Password Filtering – Updated to clarify enpasflt.dll is provided as an option but must be tested in particular environments. Site is responsible for having password complexity software. - V-14262 IPv6 Transition – corrected registry value for disabling all interfaces to 0xFF.	27 August 2010