WINDOWS SERVER 2008 R2
MEMBER SERVER (MS) STIG
REVISION HISTORY

Version 1, Release 25

26 January 2018

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R25	- Windows 2008 R2 MS STIG	- V-15823 - Clarified noted exceptions. - V-26531 - Removed Audit Computer Account Management Success, applies to Domain Controllers only. - V-26532 - Removed requirement Audit Computer Account Management Failures to align with Windows 2016 STIG. - V-26554 - Removed requirement Audit Security State Change Failures to align with Windows 2016 STIG. - V-78057 - Added Audit Account Lockout Successes to align with Windows 2016 STIG. - V-78059 - Added Audit Account Lockout Failures to align with Windows 2016 STIG. - V-57633 - Added Audit Authorization Policy Change Successes to align with Windows 2016 STIG. - V-78061 - Added Audit Other System Events Successes to align with Windows 2016 STIG. - V-78063 - Added Audit Other System Events Failures to align with Windows 2016 STIG. **Windows 2008 R2 MS Benchmark, V1R28:** - V-26531 - Removed OVAL content, requirement removed from the manual STIG. - V-26532 - Removed OVAL content, requirement removed from the manual STIG. - V-26554 - Removed OVAL content, requirement removed from the manual STIG. - V-57633 - Added new OVAL content for the Audit Authorization Policy Change (Success). - V-78057 - Added new OVAL content for the Audit Account Lockout (Success). - V-78059 - Added new OVAL content for the Audit Account Lockout (Failure). - V-78061 - Added new OVAL content for the Audit Other System Events (Success). - V-78063 - Added new OVAL content for the Audit Other System Events (Failure).	26 January 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R24	- Windows 2008 R2 MS 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 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. **Windows 2008 R2 MS Benchmark, V1R27:** - Removed OVAL content for the following as requirement has been removed from the STIG: V-26475, V-26477, V-26502, V-26505 - 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 and not specifically for other defaults.	27 October 2017
V1R23	- Windows 2008 R2 MS STIG	- V-1098 - Updated reset account lockout counter to 15 minutes or greater. - V-1099 - Updated account lockout duration to 15 minutes or greater.	28 July 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1112 - Corrected typo referring to built-in admin account as disabled. - V-1120 - Updated Check to more accurately verify FTP configuration. - V-1121 - Updated Check to more accurately verify FTP configuration. - V-3337 - Removed exception note; no longer applicable. - V-14243 - Updated Rule Title to more accurately reflect requirement. - V-26602 - Clarified Rule Title; service must be disabled unless required. - V-36439 - Updated Fix to use custom admin template instead of direct registry update. - V-36451 - Clarified requirement; policy required, technical means to enforce. **Windows 2008 R2 MS Benchmark, V1R26:** - 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 - Added OVAL to check permissions on Winreg registry key. - V-26070 - Added OVAL to check permissions on Winlogon registry key.	
V1R22	- Windows 2008 R2 MS 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.	28 April 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-73519 - Added requirement to disable Server Message Block (SMB) v1 on the SMB server. - V-73523 - Added requirement to disable Server Message Block (SMB) v1 on the SMB client. **Windows 2008 R2 MS Benchmark, V1R25:** - 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.	
V1R21	- Windows 2008 R2 MS STIG	- V-26496 - Updated to include application exception. - V-32274 - Updated expired certificate with replacement. - V-72753 - Added requirement to disable WDigest. - V-14262 - Removed requirement to disable IPv6. - 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-4446, V-14254, V-15719, V-16005, V-26471, V-26491, V-26495. **Windows 2008 R2 MS Benchmark, V1R24:** - 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:	27 January 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-1158, V-1159, V-3457, V-3458, V-14254, V-14262, V-15714, V-15715, V-15717, V-15719, V-16005, V-26471, V-26491, V-26495, V-56511, V-57455, V-57463, V-57465, V-57467, V-57469, V-57471, V-57473, V-57475, V-57477, V-57479.	
V1R20	- Windows 2008 R2 MS STIG	- V-1155 - Updated to allow "Local account and member of Administrators group". - V-15505 - Updated for v5 of McAfee agent. - V-32272 - 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-56511 - Clarified Windows Error Reporting service requirement on server core installations. - V-57457 - Clarified requirement for location of Windows Error Reporting data. - V-57461 - Removed Windows Error Reporting port requirement, not security related. **Windows 2008 R2 MS Benchmark, V1R23:** - V-1155 - Updated to allow "Local account and member of Administrators group". - V-26604 - Added new OVAL content. - V-26605 - Added new OVAL content. - V-26606 - Added new OVAL content. - V-32272 - Updated OVAL to reference current certificates. - V-32274 - Updated OVAL to reference current certificates. - V-40237 - Updated OVAL to reference current certificates.	28 October 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R19	- Windows 2008 R2 MS STIG	- V-1107 - Clarified with regard to selection of 24 for password history. - V-1112 - Clarified Check, replaced DumpSec with PowerShell query. - V-1155 - Updated to require use of "Local account" to deny access on member servers. - V-16006 - Removed general requirement, specific service requirements are included in STIG. - V-26473 - Clarified requirement, added separate Rule for member servers. - V-26486 - Updated to require use of "Local account" to deny access on member servers. - 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. **Windows 2008 R2 MS Benchmark, V1R22:** - V-1155 - Modified OVAL content to remove DenyNetworkAccess/DeniedNetworkAccess groups. - V-26473 - Split rules for DC/MS, clarification of MS allowed exceptions. - V-26486 - Modified OVAL content to remove DenyNetworkAccess/DeniedNetworkAccess groups. - V-26600 - Added new OVAL content. - V-26602 - Added new OVAL content. - V-45589 - Disabled rule in OVAL.	22 July 2016
V1R18	- Windows 2008 R2 MS 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.	22 April 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1150 - Raised requirement for Windows built-in password complexity to a CAT II. - V-1152 - Clarified requirement to maintain the default permissions. - V-14226 - Removed references to SAMI data. - 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-32282 - Clarified requirement to maintain the default permissions. - V-36669 - Removed requirement due to excessive event generation. **Windows 2008 R2 MS Benchmark, V1R20:** - V-1155 - Updated OVAL to properly check for domain membership. - V-7002 - Added OVAL. - V-15671 - Disabled Rule. - V-26483 - Updated OVAL to properly check for domain membership. - V-26484 - Updated OVAL to properly check for domain membership. - V-26485 - Updated OVAL to properly check for domain membership. - V-26486 - Updated OVAL to properly check for domain membership. - V-26544 - Disabled Rule. - V-26545 - Disabled Rule.	
V1R17	- Windows 2008 R2 MS STIG	- V-1074 - Removed Symantec from requirement. - V-1077 - Updated to allow default permissions. - V-1137 - Removed requirement. - V-14250 - Removed requirement. - V-14254 - Retargeted to member servers only.	23 October 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-26496 - Updated "Manage auditing and security log" user right to allow "Administrators". - V-36663 - Clarification for virtual machines. - V-36664 - Clarification for virtual machines. - V-40195 - Clarification for virtual machines. - 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-4444, V-21956, V-21964. - Removed EMET requirements: V-36701, V-36702, V-36703, V-36704, V-36705, V-36706, V-39137. **Windows 2008 R2 MS Benchmark, V1R19:** - V-15823 Matched file extensions case insensitivity. - V-26496 Updated "Manage auditing and security log" user right: Allow "Administrators". - V-36701 Removed requirement. - V-36702 Removed requirement. - V-36703 Removed requirement. - V-36704 Removed requirement. - V-36705 Removed requirement. - V-36706 Removed requirement. - V-39137 Removed requirement. - V-40237 Updated to search an additional path when certificate is installed via group policy. - Removed unreferenced OVAL content.	
V1R16	- Windows 2008 R2 MS STIG	- Added Section 1.6 Other Considerations to the STIG Overview document. - 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.	24 July 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- The following have been updated to add Fix details as well as miscellaneous text updates: V-1089, V-1097, V-1098, V-1099, V-1104, V-1105, V-1107, V-1112, V-1113, V-3339, V-4443, V-21954, V-26469, V-26476, V-26477, V-26478, V-26481, V-26487, V-26488, V-26491, V-26493, V-26496, V-26497, V-26498, V-26499, V-26500, V-26501, V-26502, V-26505. - The following User Rights requirements have been updated to remove Documentable tags and/or add Severity Overrides for exceptions: V-1102, V-18010, V-26470, V-26471, V-26472, V-26474, V-26475, V-26479, V-26480, V-26489, V-26490, V-26492, V-26494, V-26495, V-26503, V-26504, V-26506. - V-26473 - Changed Documentable to note. - V-26482 - Updated to allow for "Virtual Machines" when Hyper-V role is installed. **Windows 2008 R2 MS Benchmark, V1R18:** - 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-4445 Modified check against registry value. - V-26482 Added Hyper-V check. - V-32272 Added registry check. - V-32274 Added registry check. - V-39137 Updated check for EMET.	
V1R15	- Windows 2008 R2 MS STIG	- STIG Support Helpdesk email has been updated to disa.stig_spt@mail.mil. - DISA Field Security Operations (FSO) changed to DISA.	24 April 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-1090 - Requirement is NA for non domain joined systems. - 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, retargeted to member servers only. - 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. - 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 2008 R2 MS Benchmark, V1R17:** - 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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.	
V1R14	- Windows 2008 R2 MS STIG	- STIGs previously bundled in the Windows Server packages have been separated into individual packages (e.g., Member Server, Domain Controller, AD Domain, and AD Forest). - Windows Error Reporting requirements have been updated/added to enable error reporting and maintain locally. STIG IDs have been updated to organize 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.	23 January 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - V-26486 - Deny log on through Remote Desktop \ Terminal Services. - V-45589 - Define group for deny rights. - V-1137 - Access Restrictions to Logs - Corrected reference to V-26496. - V-14253 - RPC - Unauthenticated RPC Clients - Retargeted to member servers only. - V-14262 - IPv6 Transition - Updated with additional registry value. - V-15682 - RSS Attachment Downloads - Updated for policy name change (depending on IE version). **Windows 2008 R2 MS Benchmark, V1R16:** - 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - 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-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-32274 - Added OVAL content for the "DoD Interoperability Root CA 1 to DoD Root CA 2 cross-certificate" requirement.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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.	
V1R13	- Windows 2008 R2 STIG	- Control Correlation Identifiers (CCIs) added to requirements. - 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. **Member Server Specific Requirements:** - V-1127 - Administrator Group Membership - Clarification of accounts allowed for AD admin platforms. **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
V1R12	- Windows 2008 R2 STIG	- The following requirements have been removed as not affecting this version of Windows:	25 July 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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-36439 Local Admin Accounts Filtered Token Policy - Retargeted to member servers only, not applicable to domain controllers. **Benchmark/Oval Updates:** - V-1080 - Removed requirement from benchmark due to inability to verify audit settings when configured via group policy in lieu of command line. - V-3469 - Updated OVAL content to allow for registry value to not exist. - V-34974 - Added OVAL content for the requirement.	
V1R11	- Windows 2008 R2 STIG	- 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. **Member Server Specific Requirements:** - V-1127 Administrators Group Membership - Added comment related to AD admin platforms. - V-1155 Deny access from the network - Updated to incorporate	25 April 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		"DenyNetworkAccess" group defined in V-45589. Added comment related to AD admin platforms. - V-26470 Access this computer from the network - Added comment related to AD admin platforms. - V-26485 Deny log on locally - Added comment related to AD admin platform. - 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. **Benchmark/Oval Updates:** - V-1090 Updated content by removing unnecessary extended definitions. - V-1093 Updated content by removing unnecessary extended definitions. - V-1151 Updated content by removing unnecessary extended definitions. - V-3469 Updated content by removing unnecessary extended definitions. - V-4446 Updated content by removing unnecessary extended definitions. - V-15687 Updated content by removing unnecessary extended definitions. - V-15722 Updated content by removing unnecessary extended definitions. - 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-39137 Updated content to verify EMET version using the registry in lieu of the version of the EMET DLL file.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Member Server Specific Requirements: - V-1155 Added automated content for the vulnerability. - V-26846 Added automated content for the vulnerability. - V-45589 Added automated content for the vulnerability.	
V1R10	- Windows 2008 R2 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-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. - V-32273 External CA Root Certificate - Removed from STIG. - V-15996 TS/RDS Clipboard Redirection - Removed from STIG. **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-15823 Software Certificate Installation Files – Content was previously removed from the benchmark due to an issue when using SCC. The issue has been corrected.	24 January 2014
V1R9	- Windows 2008 R2 STIG	- The following sections were removed from the Overview document. Deviations or exceptions must follow standard adjudication	25 October 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		process. IAVMs are no longer included with Windows STIGs. - 3.2 ACL Deviations - 3.3 Application Exceptions - 3.5 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-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-36701 EMET ASLR Configuration - Content added for the requirement. - 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.	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-36706 EMET System-wide SEHOP Configuration - Content added for the requirement. - V-39137 EMET must be installed - Content added for the requirement.	
V1R8	- Windows 2008 R2 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-14250 Configure Automatic Updates - Corrected registry path for location of WSUS server. - V-18010 User Right - Debug Programs - Added Administrators as allowed. - V-36669 The system must be configured to audit Object Access - Handle Manipulation failures - Added requirement. - Requirements added for Enhanced Mitigation Experience Toolkit (EMET): - 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.	26 July 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- 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. - V-15823 Software Certificate Installation Files – Removed from benchmark. - V-18010 User Right - Debug Programs - Added Administrators as allowed.	
V1R7	- Windows 2008 R2 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. Requirements may vary between Domain Controllers and Member Servers where noted. - A section on this with a reference to a Microsoft document has been added to the STIG Overview document. - 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. **Member Server Specific Requirements:** - V-1127 Restricted Administrator Group Membership - changed to a Cat I, retargeted	29 March 2013

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		existing Rule ID to member servers, added requirement for domain member server administrator group on domain systems. - Several User Rights have been updated, restricting Domain and Enterprise Admins groups and/or local administrator accounts on domain systems. Existing Rule IDs were retargeted to Member Servers. - V-1155 Deny Access from the Network - STIG ID WINUR-000017-MS. - V-26483 Deny log on as a batch job - STIG ID WINUR-000018-MS. - V-26484 Deny log on as a service - STIG ID WINUR-000019-MS. - V-26485 Deny log on locally - STIG ID WINUR-000020-MS. - V-26486 Deny log on through Remote Desktop Services - STIG ID WINUR-000021-MS. **Benchmark/Oval Updates:** **Member Server Specific Requirements:** - 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.	
V1R6	- Windows 2008 R2 STIG	- V-1089 Legal Banner – Corrected double dash in banner text. - V-3487 Unnecessary Services – Corrected "SPP Notification Service" in default list. - 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.	26 October 2012

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V1R5	- Windows 2008 R2 STIG	- Overview Section 1.6 – Updated email address for FSO STIG Customer Support. - New Cat I Requirement: - V-32282 Active Setup Registry Permissions. - Three 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 – Changed focus to unsupported Service Packs consistent with other STIGs. 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.	27 July 2012
V1R4	- Windows 2008 R2 STIG	- V-1089 Legal Notice – Corrected registry type referenced to reg_sz.	27 April 2012
V1R3	- Windows 2008 R2 STIG	- 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”. - V-14249 TS/RDS Drive Redirection – Corrected policy path. - V-14250 Configure Automatic Updates – Updated for clarification, changed from	27 January 2012

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Documentable to not a finding when pointing to a DoD WSUS server. - V-26359 Legal Banner Title – Updated for clarification. - V-26472 Allow log on locally – Added Documentable flag. - V-26489 Generate security audits – Added Documentable flag. **Benchmark\Oval Updates:** - Added the following applicable to both Member Server and Domain Controllers: - V-1073 Approved Service Pack. - V-1080 File Auditing Configuration. - V-1089 Legal Notice. - V-1097 Bad Logon Attempts. - V-1099 Lockout Duration. - V-1157 Smart Card Removal Option. - V-3338 Anonymous Access to Named Pipes. - V-3339 Remotely Accessible Registry Paths. - V-3340 Anonymous Access to Network Shares. - V-3373 Maximum Machine Account Password Age. - V-3457 TS/RDS Time Limit for Discontinued Session. - V-3458 TS/RDS Time Limit for Idle Session. - V-4113 TCP Connection Keep-Alive Time. - V-4443 Remotely Accessible Registry Paths & Subpaths. - V-4445 Optional Subsystems. - V-4448 Group Policy Registry Policy Processing. - V-15823 Certificate Installation Files – updated to search all local drives. - V-26576 IP-HTTPS State. **Member Server Specific Requirements:**	

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Added the following Member Server check to the MS Benchmark: - V-26470 Access this computer from the network.	
V1R2	- Windows 2008 R2 STIG	- V-1077 Event Log ACLs – Added clarification to Fix on configuration of Eventlog account. - V-3487 Unnecessary Services – IP Helper service updated to Automatic in Default Installation sample. - V-6840 Password Expiration – Exception added for domain accounts that require smart card. - V-7002 Password Requirement – Exception added for domain accounts that require smart card. - V-26576 IP-HTTPS State – Correct Policy name to "IP-HTTPS State". - V-26603 IP Helper Service Disabled – Removed.	28 October 2011