CENTER FOR INTERNET SECURITY

CIS Microsoft Internet Explorer 11

v1.0.0 - 12-01-2014

http://benchmarks.cisecurity.org

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document provides prescriptive guidance for establishing a secure configuration posture for Microsoft Internet Explorer 11. This guide was tested against Microsoft Internet Explorer 11 running on Microsoft Windows 8. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Internet Explorer 11.

Consensus Guidance

This benchmark was created using a consensus review process comprised subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not inhibit the utility of the technology beyond acceptable means.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to Microsoft's Aaron Margosis, Rick Munck, and the rest of the Security Compliance Manager teams for their collaboration developing the configuration recommendations contained in this document.

Recommendations

1 Anti-Malware

1.1 Set 'Turn on Enhanced Protected Mode' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Enhanced Protected Mode provides additional protection against malicious websites by using 64-bit processes on 64-bit versions of Windows. For computers running Windows 8 and above, Enhanced Protected Mode also limits the locations Internet Explorer can read from in the registry and the file system.

If you enable this policy setting, Enhanced Protected Mode will be turned on. Any zone that has Protected Mode enabled will use Enhanced Protected Mode. Users will not be able to disable Enhanced Protected Mode.

If you disable this policy setting, Enhanced Protected Mode will be turned off. Any zone that has Protected Mode enabled will use the version of Protected Mode introduced in Internet Explorer 7 for Windows Vista.

If you do not configure this policy, users will be able to turn on or turn off Enhanced Protected Mode on the Advanced tab of the Internet Options dialog. The recommended state for this setting is: `Enabled`.

Rationale:

Enhanced Protected Mode provides additional protection against malicious websites by using 64-bit processes on 64-bit versions of Windows. For computers running Windows 8 and above, Enhanced Protected Mode also limits the locations Internet Explorer can read from in the registry and the file system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\Isolation
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Turn on Enhanced Protected Mode
```

Impact:

If you enable this policy setting, Enhanced Protected Mode will be turned on. Any zone that has Protected Mode enabled will use Enhanced Protected Mode. Users will not be able to disable Enhanced Protected Mode.
If you disable this policy setting, Enhanced Protected Mode will be turned off. Any zone that has Protected Mode enabled will use the version of Protected Mode introduced in Internet Explorer 7 for Windows Vista.

If you do not configure this policy, users will be able to turn on or turn off Enhanced Protected Mode on the Advanced tab of the Internet Options dialog.

1.2 Set 'Allow software to run or install even if the signature is invalid' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

Microsoft ActiveX® controls and file downloads often have digital signatures attached that help certify the file's integrity and the identity of the signer (creator) of the software. Such signatures help ensure that unmodified software is downloaded and that you can identify active signers to determine whether you trust them enough to run their software.

The Allow software to run or install even if the signature is invalid setting allows you to manage whether downloaded software can be installed or run by users even though the signature is invalid. An invalid signature might indicate that someone has tampered with the file. If you enable this policy setting, users will be prompted to install or run files with an invalid signature. If you disable this policy setting, users cannot run or install files with an invalid signature.

Note: Some legitimate software and controls may have an invalid signature and still be OK. You should carefully test such software in isolation before you allow it to be used on your organization's network. The recommended state for this setting is: `Disabled`.

Rationale:

Microsoft ActiveX® controls and file downloads often have digital signatures attached that certify the file's integrity and the identity of the signer (creator) of the software. Such signatures help ensure that unmodified software is downloaded and that you can positively identify the signer to determine whether you trust them enough to run their software. The validity of unsigned code cannot be ascertained.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Download\RunInvalidSignatures
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Allow software to run or install even if
the signature is invalid
```

Impact:

Some legitimate software and controls may have an invalid signature. You should carefully test such software in isolation before it is allowed to be used on your organization's network.

Default Value:

Disabled

1.3 Set 'Prevent Bypassing SmartScreen Filter Warnings' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

The SmartScreen Filter prevents users from navigating to and downloading from sites known to host malicious content, including Phishing or malicious software attacks. If you enable this policy setting, the user is not permitted to navigate to sites identified as unsafe by the SmartScreen Filter. If you disable this policy setting or do not configure it, the user can ignore SmartScreen Filter warnings and navigate to unsafe sites. The recommended state for this setting is: `Enabled`.

Rationale:

If this setting is enabled and the SmartScreen Filter is active, the user can ignore a SmartScreen Filter warning and navigate to a site determined to be unsafe.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\PhishingFilter\PreventOverride
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Prevent Bypassing SmartScreen Filter Warnings
```

Impact:

Users cannot navigate to sites detected as unsafe by the SmartScreen Filter.

Default Value:

Disabled

1.4 Set 'Prevent bypassing SmartScreen Filter warnings about files that are not commonly downloaded from the Internet' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether the user can bypass warnings from SmartScreen Filter. SmartScreen Filter warns the user about executable files that Internet Explorer users do not commonly download from the Internet.

If you enable this policy setting, SmartScreen Filter warnings block the user.

If you disable or do not configure this policy setting, the user can bypass SmartScreen Filter warnings. The recommended state for this setting is: `Enabled`.

Rationale:

The SmartScreen Filter prevents users from navigating to and downloading from sites known to host malicious content, including Phishing or malicious software attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\PhishingFilter\PreventOverrideAppRepUnknown
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Prevent bypassing SmartScreen Filter warnings about files that are not
commonly downloaded from the Internet
```

Impact:

If you enable this policy setting, the user is not permitted to navigate to sites identified as unsafe by the SmartScreen Filter. If you disable this policy setting or do not configure it, the user can ignore SmartScreen Filter warnings and navigate to unsafe sites.

1.5 Configure 'Do not allow users to enable or disable add-ons' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users have the ability to allow or deny add-ons through Add-On Manager. If you enable this policy setting, users cannot enable or disable add-ons through Add-On Manager. The only exception occurs if an add-on has been specifically entered into the 'Add-On List' policy setting in such a way as to allow users to continue to manage the add-on. In this case, the user can still manage the add-on through the Add-On Manager. If you disable or do not configure this policy setting, the appropriate controls in the Add-On Manager will be available to the user. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

Users often choose to install add-ons that are not permitted by an organization's security policy. Such add-ons can pose a significant security and privacy risk to your network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Restrictions\NoExtensionManagement
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Do not allow users to enable or disable add-ons
```

Impact:

When the Do not allow users to enable or disable add-ons setting is enabled, users will not be able to enable or disable their own Internet Explorer add-ons. If your organization uses add-ons, this configuration may affect their ability to work.

Default Value:

Disabled

1.6 Set 'Disable Save this program to disk option' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents users from saving a program or file that Internet Explorer has downloaded to the hard disk. If you enable this policy setting, users cannot save programs to disk with the Save this program to disk option. The program file will not download, and the user is informed that the command is not available. The recommended state for this setting is: `Enabled`.

Rationale:

Users could download and execute hostile code from Web sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\Software\Policies\Microsoft\Internet
Explorer\Restrictions\NoSelectDownloadDir
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
User Configuration\Administrative Templates\Windows Components\Internet
Explorer\Browser menus\Disable Save this program to disk option
```

Impact:

Users will be unable to click the Save This Program to Disk button to download program files.

Default Value:

Disabled

2 ActiveX Settings

2.1 Set 'Prevent per-user installation of ActiveX controls' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to prevent the installation of ActiveX controls on a per-user basis. If you enable this policy setting, ActiveX controls cannot be installed on a per-user basis. If you disable or do not configure this policy setting, ActiveX controls can be installed on a per-user basis. The recommended state for this setting is: `Enabled`.

Rationale:

Per-user installation of ActiveX controls is a convenient feature that many organizations may want to leverage. One benefit is that even if the user installs a control that includes a malicious payload its impact will be limited to the privileges of the user who installed it. Nevertheless, restricting the installation of ActiveX controls to administrators and using the ActiveX Installer Service or some other centralized software deployment tool is a more effective method for avoiding malware.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Security\ActiveX\BlockNonAdminActiveXInstall
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Prevent per-user installation of ActiveX controls
```

Impact:

If you enable this policy setting, ActiveX controls cannot be installed on a per-user basis. If you disable or do not configure this policy setting, ActiveX controls can be installed on a per-user basis.

2.2 Set 'Specify use of ActiveX Installer Service for installation of ActiveX controls' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to specify how ActiveX controls are installed. If you enable this policy setting, ActiveX controls are installed only if the ActiveX Installer Service is present and has been configured to allow the installation of ActiveX controls. If you disable or do not configure this policy setting, ActiveX controls, including per-user controls, are installed through the standard installation process. The recommended state for this setting is: `Enabled`.

Rationale:

The ActiveX Installer Service can be a more secure method for deploying ActiveX controls needed for business purposes than allowing users to download and install them because organizations can ensure they are legitimate and scan them for malware prior to deployment.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AxInstaller\OnlyUseAXISForActiv
eXInstall
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Specify use of ActiveX Installer Service for installation of ActiveX controls
```

Impact:

If you enable this policy setting, ActiveX controls are installed only if the ActiveX Installer Service is present and has been configured to allow the installation of ActiveX controls. If you disable or do not configure this policy setting, ActiveX controls, including per-user controls, are installed through the standard installation process.

2.3 Set 'Turn on ActiveX Filtering' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the ActiveX Filtering feature for websites running ActiveX controls. The user can choose to turn off ActiveX Filtering for specific websites so that its ActiveX controls can run properly. If you enable this policy setting, ActiveX Filtering will be enabled by default for the user. The user cannot turn off ActiveX Filtering although they may add per-site exceptions. If you disable this policy setting or do not configure it, ActiveX Filtering will not be enabled by default for the user. The user can turn ActiveX Filtering on or off. The recommended state for this setting is: `Enabled`.

Rationale:

ActiveX Filtering allows you to make an informed decision about every ActiveX control you run by giving you the ability to block ActiveX controls for all sites, and then turn them on for only the sites that you trust. This can help improve your protection against risky and unreliable ActiveX controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Safety\ActiveXFiltering\IsEnabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Turn on ActiveX Filtering
```

Impact:

If you enable this policy setting, ActiveX Filtering will be enabled by default for the user. The user cannot turn off ActiveX Filtering although they may add per-site exceptions. If you disable this policy setting or do not configure it, ActiveX Filtering will not be enabled by default for the user. The user can turn ActiveX Filtering on or off.

Default Value:

Disabled

2.4 Set 'Turn off ActiveX opt-in prompt' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to turn off the ActiveX opt-in prompt. The ActiveX opt-in prevents Web sites from loading any COM object without prior approval. If a page attempts to load a COM object that Internet Explorer has not used before, an Information bar will appear asking the user for approval. If you enable this policy setting, the ActiveX opt-in prompt will not appear. Internet Explorer does not ask the user for permission to load a control, and will load the ActiveX if it passes all other internal security checks. If you disable or do not configure this policy setting, the ActiveX opt-In prompt will appear. The recommended state for this setting is: `Disabled`.

Rationale:

If the user were to enable this setting the ActiveX opt-in prompt would be disabled and malicious ActiveX controls could be executed without the user's knowledge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Ext\NoFirsttimeprompt
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Turn off ActiveX opt-in prompt
```

Impact:

Enabling this setting would allow the possibility of malicious ActiveX controls to be executed without the user's knowledge.

Default Value:

Not Configured

2.5 Set 'Do not allow ActiveX controls to run in Protected Mode when Enhanced Protected Mode is enabled' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents ActiveX controls from running in Protected Mode when Enhanced Protected Mode is enabled. When a user has an ActiveX control installed that is not compatible with Enhanced Protected Mode and a website attempts to load the control, Internet Explorer notifies the user and gives the option to run the website in regular Protected Mode. This policy setting disables this notification and forces all websites to run in Enhanced Protected Mode.

Enhanced Protected Mode provides additional protection against malicious websites by using 64-bit processes on 64-bit versions of Windows. For computers running Windows 8 and above, Enhanced Protected Mode also limits the locations Internet Explorer can read from in the registry and the file system.

When Enhanced Protected Mode is enabled, and a user encounters a website that attempts to load an ActiveX control that is not compatible with Enhanced Protected Mode, Internet Explorer notifies the user and gives the option to disable Enhanced Protected Mode for that particular website.

If you enable this policy setting, Internet Explorer will not give the user the option to disable Enhanced Protected Mode. All Protected Mode websites will run in Enhanced Protected Mode.

If you disable or do not configure this policy setting, Internet Explorer notifies users and provides an option to run websites with incompatible ActiveX controls in regular Protected Mode. This is the default behavior. The recommended state for this setting is: `Enabled`.

Rationale:

Enhanced Protected Mode provides additional protection against malicious websites by using 64-bit processes on 64-bit versions of Windows. For computers running Windows 8 and above, Enhanced Protected Mode also limits the locations Internet Explorer can read from in the registry and the file system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\DisableEPMCompat
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Do not allow ActiveX controls to run in
Protected Mode when Enhanced Protected Mode is enabled
```

Impact:

When Enhanced Protected Mode is enabled, and a user encounters a website that attempts to load an ActiveX control that is not compatible with Enhanced Protected Mode, Internet Explorer notifies the user and gives the option to disable Enhanced Protected Mode for that particular website.

If you enable this policy setting, Internet Explorer will not give the user the option to disable Enhanced Protected Mode. All Protected Mode websites will run in Enhanced Protected Mode.

If you disable or do not configure this policy setting, Internet Explorer notifies users and provides an option to run websites with incompatible ActiveX controls in regular Protected Mode. This is the default behavior.

3 Browsing History

3.1 Configure 'Prevent deleting websites that the user has visited' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents the user from deleting the history of websites that he or she has visited. This feature is available in the Delete Browsing History dialog box.

If you enable this policy setting, websites that the user has visited are preserved when he or she clicks Delete. If you disable this policy setting, websites that the user has visited are deleted when he or she clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve visited websites when he or she clicks Delete.

If the "Prevent access to Delete Browsing History" policy setting is enabled, this policy setting is enabled by default. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

If users can delete websites they have visited it will be easier for them to hide evidence that they have visited unauthorized sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Privacy\CleanHistory
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Delete Browsing History\Prevent deleting websites that the user has visited
```

Impact:

If you enable this policy setting, websites that the user has visited are preserved when he or she clicks Delete.

If you disable this policy setting, websites that the user has visited are deleted when he or she clicks Delete.

If you do not configure this policy setting, the user can choose whether to delete or preserve visited websites when he or she clicks Delete.

If the "Prevent access to Delete Browsing History" policy setting is enabled, this policy setting is enabled by default.

3.2 Configure 'Prevent Deleting Cookies' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting is used to prevent users from deleting cookies. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, cookies will be preserved when the user clicks Delete. If you disable this policy setting, cookies will be deleted when the user clicks Delete. If you do not configure this policy setting, the user will be able to choose whether to delete or preserve cookies when the user clicks Delete. If the "Turn off Delete Browsing History functionality" policy is enabled, this policy is enabled by default. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

If a user is suspected of visiting unauthorized website the information stored in the data cookies could be useful in verifying where he or she went online.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Privacy\CleanCookies
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Delete Browsing History\Prevent Deleting Cookies
```

Impact:

If you enable this policy setting, users will not be able to delete cookies. If you disable or do not configure this policy setting, users will be able to delete cookies.

Default Value:

Disabled

3.3 Set 'Disable "Configuring History"' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This setting specifies the number of days that Internet Explorer keeps track of the pages viewed in the History List. The recommended state for this setting is: `Enabled`.

Rationale:

If users can delete their browsing history it will be easier for them to hide evidence that they have visited unauthorized sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control Panel\History
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Delete Browsing History\Disable "Configuring History"
```

Impact:

If you enable this policy setting, a user cannot set the number of days that Internet Explorer keeps track of the pages viewed in the History List. You must specify the number of days that Internet Explorer keeps track of the pages viewed in the History List. Users will not be able to delete browsing history. If you disable or do not configure this policy setting, a user can set the number of days that Internet Explorer keeps track of the pages viewed in the History List and has the freedom to Delete Browsing History.

Default Value:

Disabled

3.4 Set 'Days to keep pages in History' to '40' (Scored)

Profile Applicability:

- Level 1

Description:

This setting specifies the number of days that Internet Explorer keeps track of the pages viewed in the History List. The recommended state for this setting is: `40`.

Rationale:

The browsing history may increase an organization' s ability to determine if a user has visited unauthorized sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Url History\DaysToKeep
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `40`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Delete Browsing History\Disable "Configuring History": Days to keep pages in History
```

Impact:

If you enable this policy setting, a user cannot set the number of days that Internet Explorer keeps track of the pages viewed in the History List. You must specify the number of days that Internet Explorer keeps track of the pages viewed in the History List. Users will not be able to delete browsing history. If you disable or do not configure this policy setting, a user can set the number of days that Internet Explorer keeps track of the pages viewed in the History List and has the freedom to Delete Browsing History.

Default Value:

Not Configured

3.5 Configure 'Prevent Deleting Temporary Internet Files' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting is used to prevent users from deleting temporary Internet files. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, temporary Internet files will be preserved when the user clicks Delete. If you disable this policy setting, temporary Internet files will be deleted when the user clicks Delete. If you do not configure this policy setting, the user will be able to choose whether to delete or preserve temporary Internet files when the user clicks Delete. If the `Turn off Delete Browsing History functionality` policy is enabled, this policy is enabled by default. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

If a user is suspected of visiting unauthorized website the information stored in the Temporary Internet Files folder could be useful in verifying where he or she went online.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Privacy\CleanTIF
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Delete Browsing History\Prevent Deleting Temporary Internet Files
```

Impact:

If you enable this policy setting, users will not be able to delete temporary Internet files. If you disable or do not configure this policy setting, users will be able to delete temporary Internet files.

Default Value:

Not Configured

3.6 Configure 'Allow deleting browsing history on exit' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows the automatic deletion of specified items when the last browser window closes. The preferences selected in the Delete Browsing History dialog box (such as deleting temporary Internet files, cookies, history, form data, and passwords) are applied, and those items are deleted.

If you enable this policy setting, deleting browsing history on exit is turned on.
If you disable this policy setting, deleting browsing history on exit is turned off.
If you do not configure this policy setting, it can be configured on the General tab in Internet Options.

If the "Prevent access to Delete Browsing History" policy setting is enabled, this policy setting has no effect. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

If users can delete their browsing history it will be easier for them to hide evidence that they have visited unauthorized sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Privacy\ClearBrowsingHistoryOnExit
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Delete Browsing History\Allow deleting browsing history on exit
```

Impact:

If you enable this policy setting, deleting browsing history on exit is turned on.

If you disable this policy setting, deleting browsing history on exit is turned off.

If you do not configure this policy setting, it can be configured on the General tab in Internet Options.

If the "Prevent access to Delete Browsing History" policy setting is enabled, this policy setting has no effect.

3.7 Set 'Prevent access to Delete Browsing History' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents the user from performing actions which will delete browsing history. For more information on browsing history Group Policy settings, see "Group Policies Settings in Internet Explorer 10" in the TechNet technical library.

If you enable this policy setting, the user cannot access the Delete Browsing History dialog box. Starting with Windows 8, users cannot click the Delete Browsing History button on the Settings charm.

If you disable or do not configure this policy setting, the user can access the Delete Browsing History dialog box. Starting with Windows 8, users can click the Delete Browsing History button on the Settings charm. The recommended state for this setting is: `Enabled`.

Rationale:

If users can delete their browsing history it will be easier for them to hide evidence of visiting unauthorized sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control
Panel\DisableDeleteBrowsingHistory
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Delete Browsing History\Prevent access to Delete Browsing History
```

Impact:

If you enable this policy setting, the user cannot access the Delete Browsing History dialog box. Starting with Windows 8, users cannot click the Delete Browsing History button on the Settings charm.

If you disable or do not configure this policy setting, the user can access the Delete Browsing History dialog box. Starting with Windows 8, users can click the Delete Browsing History button on the Settings charm.

3.8 Configure 'Turn off InPrivate Browsing' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to disable the InPrivate Browsing feature. InPrivate Browsing prevents Internet Explorer from storing data about a user's browsing session. This includes cookies, temporary Internet files, history, and other data. If you enable this policy setting, InPrivate Browsing will be disabled. If you disable this policy setting, InPrivate Browsing will be available for use. If you do not configure this setting, InPrivate

Browsing can be turned on or off through the registry. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

InPrivate browsing can increase the privacy of a user who is browsing websites, disabling this setting ensures that users will be able to use the feature. On the other hand, organizations that closely monitor their users online activities may wish to disable InPrivate browsing to ensure they are able to collect detailed information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Privacy\EnableInPrivateBrowsing
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Privacy\Turn off InPrivate Browsing
```

4 Component Updates

4.1 Configure 'URL to be displayed for updates:' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents the user from changing the default URL for checking updates to Internet Explorer and Internet Tools. If you enable this policy setting, the user cannot change the URL that is displayed for checking updates to Internet Explorer and Internet Tools. You must specify this URL. If you disable or do not configure this policy setting, the user can change the URL that is displayed for checking updates to Internet Explorer and Internet Tools. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

Enabling this setting will ensure that updates are downloaded from sites specified by the organization's information technology team.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Main\Update_Check_Page
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Settings\Component Updates\Periodic check for updates to Internet
Explorer and Internet Tools\Prevent changing the URL for checking updates to Internet
Explorer and Internet Tools: URL to be displayed for updates:
```

Impact:

If you enable this policy setting, the user cannot change the URL that is displayed for checking updates to Internet Explorer and Internet Tools. You must specify this URL. If you

disable or do not configure this policy setting, the user can change the URL that is displayed for checking updates to Internet Explorer and Internet Tools.

4.2 Set 'Update check interval (in days):' to 'Enabled:30' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents the user from specifying the update check interval. The default value is 30 days. If you enable this policy setting, the user cannot specify the update check interval. You must specify the update check interval. If you disable or do not configure this policy setting, the user can specify the update check interval. The recommended state for this setting is: `Enabled:30`.

Rationale:

Enabling this setting will ensure that updates are downloaded at the interval specified by the organization's information technology team.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Main\Update_Check_Interval
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Settings\Component Updates\Periodic check for updates to Internet
Explorer and Internet Tools\Prevent specifying the update check interval (in days)
```

Then set the `Update check interval (in days):` option to `30`.

Impact:

If you enable this policy setting, the user cannot specify the update check interval. You must specify the update check interval. If you disable or do not configure this policy setting, the user can specify the update check interval.

4.3 Configure 'Automatically check for Internet Explorer updates' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Internet Explorer checks the Internet for newer versions. When Internet Explorer is set to do this, the checks occur approximately every 30 days, and users are prompted to install new versions as they become available. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

If you enable this policy setting, Internet Explorer checks the Internet for a new version approximately every 30 days and prompts the user to download new versions when they are available. Newer versions might not comply to the Internet Explorer version requirements of your organization.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\NoUpdateCheck
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`**.**

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Automatically check for Internet
Explorer updates
```

Impact:

If you enable this policy setting, Internet Explorer checks the Internet for a new version approximately every 30 days and prompts the user to download new versions when they are available. If you disable this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them.

Default Value:

Disabled

4.4 Configure 'Install new versions of Internet Explorer automatically' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting configures Internet Explorer to automatically install new versions of Internet Explorer when they are available. If you enable this policy setting, automatic upgrade of Internet Explorer will be turned on.
If you disable this policy setting, automatic upgrade of Internet Explorer will be turned off. If you do not configure this policy, users can turn on or turn off automatic updates from the About Internet Explorer dialog. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

There's no known vulnerability at this time, but organizations that manage software and patches may want to disable the setting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Main\EnableAutoUpgrade
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Install new versions of Internet Explorer automatically
```

5 Certificates and Protocols

5.1 Set 'Turn off Encryption Support' to 'Use TLS 1.1 and TLS 1.2' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to turn off support for Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0 or SSL 3.0 in the browser. TLS and SSL are protocols for protecting communication between the browser and the target server. When the browser attempts to set up a protected communication with the target server, the browser and server negotiate which protocol and version to use. The browser and server attempt to match each other's list of supported protocols and versions and pick the most preferred match. If you enable this policy setting, the browser will or will not negotiate an encryption tunnel with the encryption methods you select through the drop down list. If you disable or do not configure this policy setting, the user can select which encryption method the browser will support. The recommended state for this settings is `Use TLS 1.1 and TLS 1.2. Only use TLS 1.2` also conforms with this guidance.

Rationale:

Risk is reduced by preventing Internet Explorer from communicating over protocols, such as SSL v2.0 and SSL v3.0, that suffer from known practical attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\SecureProtocols
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Use TLS 1.1 and TLS 1.2`

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Turn off Encryption Support: Secure
Protocol combinations
```

Impact:

Determines the encryption protocols that may be used. One of the designated protocols needs to be active on both sides of the connection for encryption to function correctly.

Default Value:

Disabled

5.2 Set 'Check for server certificate revocation' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Internet Explorer will check revocation status of servers' certificates. Certificates are revoked when they have been compromised or are no longer valid, and this option protects users from submitting confidential data to a site that may be fraudulent or not secure.
If you enable this policy setting, Internet Explorer will check to see if server certificates have been revoked. If you disable this policy setting, Internet Explorer will not check server certificates to see if they have been revoked. If you do not configure this policy setting, Internet Explorer will not check server certificates to see if they have been revoked. The recommended state for this setting is: `Enabled`.

Rationale:

Certificates are revoked when they have been compromised or are no longer valid. If Internet Explorer does not check for the status of a certificate, users and this option protects users could inadvertently submit confidential data to a site that may be fraudulent or not secure.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\CertificateRevocation
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Check for server certificate revocation
```

Impact:

If you enable this policy setting, Internet Explorer will check to see if server certificates have been revoked. If you disable this policy setting, Internet Explorer will not check server certificates to see if they have been revoked.

Default Value:

Disabled

5.3 Set 'Check for signatures on downloaded programs' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Internet Explorer checks for digital signatures (which identifies the publisher of signed software and verifies it hasn't been modified or tampered with) on user computers before downloading executable programs.

If you enable this policy setting, Internet Explorer will check the digital signatures of executable programs and display their identities before downloading them to user computers.

If you disable this policy setting, Internet Explorer will not check the digital signatures of executable programs or display their identities before downloading them to user computers.

If you do not configure this policy, Internet Explorer will not check the digital signatures of executable programs or display their identities before downloading them to user computers. The recommended state for this setting is: `Enabled`.

Rationale:

Although digitally signing software does not guarantee that it includes no malware it does reduce the risk and it provides another potential path of investigation should the software include a dangerous payload.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Download\CheckExeSignatures
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page\Check for signatures on downloaded
programs
```

5.4 Set 'Turn on certificate address mismatch warning' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to turn on the certificate address mismatch security warning. When this policy setting is turned on, the user is warned when visiting Secure HTTP (HTTPS) websites that present certificates issued for a different website address. This warning helps prevent spoofing attacks. If you enable this policy setting, the certificate address mismatch warning always appears. If you disable or do not configure this policy setting, the user can choose whether the certificate address mismatch warning appears (by using the Advanced page in the Internet Control panel). The recommended state for this setting is: `Enabled`.

Rationale:

When this policy setting is turned on, the user is warned when visiting Secure HTTP (HTTPS) websites that present certificates issued for a different website address, which may help prevent spoofing attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\WarnOnBadCertRecving
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Turn on certificate address mismatch warning
```

5.5 Set 'Prevent ignoring certificate errors' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

When a user experiences Secure Socket Layer/Transport Layer Security (SSL/TLS) certificate errors such as "expired," "revoked," or "name mismatch," Internet Explorer blocks the user's ability to continue browsing the Web site. The recommended state for this setting is: `Enabled`.

Rationale:

Users who ignore certificate errors are more likely to visit unauthorized sites or sites that host malicious content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\PreventIgnoreCertErrors
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Prevent ignoring certificate errors
```

Impact:

If you enable this policy setting, the user is not permitted to continue browsing the Web site. If you disable this policy setting or do not configure it, the user may elect to ignore certificate errors and continue browsing the Web site.

Default Value:

Disabled

5.6 Set 'Disable changing certificate settings' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting removes a user's ability to change certificate settings in Internet Explorer. Certificates are used to verify the identity of software publishers. If you enable this policy setting, the certificate settings in the Certificates area of the Content tab in the Internet Options dialog box are dimmed. This policy setting also removes a user's ability to change settings that are configured through Group Policy.

Note: When this policy setting is enabled, users can still double-click the software publishing certificate (`.spc`) file to run the Certificate Manager Import Wizard. This wizard enables users to import and configure settings for certificates from software publishers that are not already configured in Internet Explorer.

Note: The Disable the Content page setting removes the Content tab from Internet Explorer in Control Panel and takes precedence over this Disable changing certificate settings configuration option. If the former setting is enabled, the latter setting is ignored. The Disable the Content page setting located in `\User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel` in the Group Policy Object Editor. The recommended state for this setting is: `Enabled`.

Rationale:

Users could import new certificates, remove approved certificates, or change settings for previously configured ones. Such occurrences could cause approved applications to fail, or unapproved software to be executed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\Software\Policies\Microsoft\Internet Explorer\Control
Panel\Certificates
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
User Configuration\Administrative Templates\Windows Components\Internet
Explorer\Disable changing certificate settings
```

Impact:

Users will be unable to change the certificate settings.

Default Value:

Disabled

6 Internet Communication Management

6.1 Set 'Turn off browser geolocation' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to disable browser geolocation support. This will prevent websites from requesting location data about the user. If you enable this policy setting, browser geolocation support is turned off. If you disable this policy setting, browser geolocation support is turned on. If you do not configure this policy setting, browser geolocation support can be turned on or off in Internet Options on the Privacy tab. The recommended state for this setting is: `Enabled`.

Rationale:

Some applications and websites may share location information with servers that the user visits, some organizations may be concerned that this location information could be exploited by a malicious user who has access to such a server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Geolocation\PolicyDisableGeolocation
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Turn off browser geolocation
```

6.2 Configure 'Turn off URL Suggestions' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting turns off URL Suggestions. URL Suggestions allow users to autocomplete URLs in the address bar based on common URLs. The list of common URLs is stored locally and is updated once a month. No user data is sent over the internet by this feature. If you enable this policy setting, URL Suggestions will be turned off. Users will not be able to turn on URL Suggestions. If you disable this policy setting, URL Suggestions will be turned on. Users will not be able to turn off URL Suggestions. If you do not configure this policy setting, URL Suggestions will be turned on. Users will be able to turn on or turn off URL Suggestions in the Internet Options dialog. By default, URL Suggestions are turned on. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

When enabled this feature will transmit some usage information to Microsoft, organizations may want to prevent the sharing of this information with Microsoft in order to protect their business data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\DomainSuggestion\Enabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Settings\AutoComplete\Turn off URL Suggestions
```

6.3 Configure 'Prevent participation in the Customer Experience Improvement Program' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents users from participating in the Customer Experience Improvement Program (CEIP). If you enable this policy setting, it prevents users from participating in the CEIP and removes the "Customer Feedback Options" menu item from the Help menu. If you disable this policy setting, users must participate in the CEIP. It also removes the "Customer Feedback Options" menu item from the Help menu. If you do not configure this policy setting, users can choose to participate in the CEIP. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

When enabled this feature will transmit some usage information to Microsoft, organizations may want to prevent the sharing of this information with Microsoft in order to protect their business data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\SQM\DisableCustomerImprovementProgram
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Prevent participation in the Customer Experience Improvement Program
```

6.4 Configure 'Turn on Suggested Sites' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the Suggested Sites feature, which recommends sites based on the user's browsing activity. Suggested Sites reports a user's browsing history to Microsoft to suggest sites the user might want to visit. If you enable this policy setting, the user will not be prompted to enable the Suggested Sites. The user's browsing history will be sent to produce suggestions. If you disable this policy setting, the entry points and functionality associated with this feature will be disabled. If you do not configure this policy setting,

users will able to enable and disable the Suggested Sites feature. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

Suggested Sites reports a user's browsing history to Microsoft to suggest sites the user might want to visit, organizations may want to prevent the sharing of this information with Microsoft in order to protect their business data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Suggested
Sites\Enabled
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Turn on Suggested Sites
```

7 Internet Explorer Process Security Features

7.1 Set 'Restrict ActiveX Install' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting provides the ability to block ActiveX control installation prompts for Internet Explorer processes. The recommended state for this setting is: `Enabled`.

Rationale:

Users often choose to install software such as ActiveX controls that are not permitted by their organization's security policy. Such software can pose significant security and privacy risks to networks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Restrict ActiveX Install\Internet Explorer Processes
```

Impact:

If you enable this policy setting, prompts for ActiveX control installations will be blocked for Internet Explorer processes. If you disable this policy setting, prompts for ActiveX control installations will not be blocked and these prompts will be displayed to users.

Note: This policy setting also blocks users from installing authorized legitimate ActiveX controls that will interfere with important system components like Windows Update. If you enable this policy setting, make sure to implement some alternate way to deploy security updates such as Windows Server Update Services (WSUS).

Default Value:

Enabled

7.2 Set 'Scripted Window Security Restrictions' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Internet Explorer allows scripts to programmatically open, resize, and reposition windows of various types. The Window Restrictions security feature restricts popup windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or obfuscate other Windows' title and status bars. If you enable this policy setting, popup windows and other restrictions apply for File Explorer and Internet Explorer processes. If you disable this policy setting, scripts can continue to create popup windows and windows that obfuscate other windows. If you do not configure this policy setting, popup windows and other restrictions apply for File Explorer and Internet Explorer processes. The recommended state for this setting is: `Enabled`.

Rationale:

The Internet Explorer Processes (Scripted Window Security Restrictions) setting restricts pop-up windows and does not allow scripts to display windows in which the title and status bars are not visible to the user or that hide other windows' title and status bars. When enabled, this policy setting help make it difficult for malicious Web sites to control your Internet Explorer windows or fool users into clicking the wrong window.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Scripted Window Security Restrictions\Internet Explorer
Processes
```

Default Value:

Enabled

7.3 Set 'Mime Sniffing Safety Feature' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

MIME sniffing is a process that examines the content of a MIME file to determine its context—whether it is a data file, an executable file, or some other type of file. This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type.

Note: This policy setting works in conjunction with, but does not replace, the Consistent MIME Handling settings. The recommended state for this setting is: `Enabled`.

Rationale:

MIME file-type spoofing is a potential threat to your organization. It is recommended that you ensure these files are consistently handled to help prevent malicious file downloads that may infect your network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Mime Sniffing Safety Feature\Internet Explorer Processes
```

Impact:

When set to Enabled, MIME sniffing will not promote a file of one type to a more dangerous file type. If you disable this policy setting, MIME sniffing configures Internet Explorer processes to allow promotion of a file from one type to a more dangerous file type. For example, a text file could be promoted to an executable file, which is dangerous because any code in the supposed text file would be executed.

Default Value:

Enabled

7.4 Set 'Notification bar' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether the Notification bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Notification bar is displayed for Internet Explorer processes. If you enable this policy setting, the Notification bar will be displayed for Internet Explorer Processes. If you disable this policy setting, the Notification bar will not be displayed for Internet Explorer processes. If you do not configure this policy setting, the Notification bar will be displayed for Internet Explorer Processes. The recommended state for this setting is: `Enabled`.

Rationale:

There's no known vulnerability at this time, however information displayed in the Notification Bar may help users to understand why files or code installs are restricted.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Notification bar\Internet Explorer Processes
```

Default Value:

Enabled

7.5 Set 'MK Protocol Security Restriction' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

The MK Protocol Security Restriction policy setting reduces attack surface area by preventing the MK protocol. Resources hosted on the MK protocol will fail. If you enable this policy setting, the MK Protocol is prevented for File Explorer and Internet Explorer, and resources hosted on the MK protocol will fail. If you disable this policy setting, applications can use the MK protocol API. Resources hosted on the MK protocol will work for the File Explorer and Internet Explorer processes. If you do not configure this policy setting, the MK Protocol is prevented for File Explorer and Internet Explorer, and resources hosted on the MK protocol will fail. The recommended state for this setting is: `Enabled`.

Rationale:

Because the MK protocol is not widely used, it should be blocked wherever it is not needed.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\MK Protocol Security Restriction\Internet Explorer
Processes
```

Default Value:

Enabled

7.6 Set 'Consistent Mime Handling' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files that are received through a Web server. The Consistent MIME Handling setting determines whether Internet Explorer requires that all file type information that is provided by Web servers be consistent. For example, if the MIME type

of a file is text/plain but the MIME data indicates that the file is really an executable file, Internet Explorer changes its extension to reflect this executable status. This capability helps ensure that executable code cannot masquerade as other types of data that may be trusted. The recommended state for this setting is: `Enabled`.

Rationale:

MIME file type spoofing is a potential threat to your organization. You should ensure that these files are consistent and properly labeled to help prevent malicious file downloads that may infect your network.

Note: This policy setting works in conjunction with, but does not replace, the MIME Sniffing Safety Features settings.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Consistent Mime Handling\Internet Explorer Processes
```

Impact:

If you enable this policy setting, Internet Explorer examines all received files and enforces consistent MIME data for them. If you disable or do not configure this policy setting, Internet Explorer does not require consistent MIME data for all received files and will use the MIME data that is provided by the file.

Default Value:

Enabled

7.7 Set 'Restrict File Download' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This setting can be used to suppress file download prompts that are not user-initiated in Internet Explorer. If you configure the Internet Explorer Processes (Restrict File Download) setting to Enabled, file download prompts that are not user-initiated are blocked for Internet Explorer processes. If you configure this policy setting to Disabled, file download prompts will occur that are not user-initiated for Internet Explorer processes. The recommended state for this setting is: `Enabled`.

Rationale:

In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on a user's hard disk drive if they click the wrong button and accept the download.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Restrict File Download\Internet Explorer Processes
```

Impact:

None. There is no legitimate reason for a Web site to start transferring a file to a user's workstation without a user request to do so.

Default Value:

Enabled

7.8 Set 'Protection From Zone Elevation' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Internet Explorer places restrictions on each Web page that it opens based on the security zone from which it originates. The recommended state for this setting is: `Enabled`.

Rationale:

These restrictions depend on the location of the Web page (such as Internet zone, Intranet zone, or Local Machine zone). Web pages on a local computer have the fewest security restrictions and reside in the Local Machine zone, malicious Web pages may attempt to elevate themselves from their current zone into another zone with higher privileges.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Protection From Zone Elevation\Internet Explorer Processes
```

Impact:

If you enable the Internet Explorer Processes (Zone Elevation Protection) setting, any zone can be protected from zone elevation by Internet Explorer processes. This approach helps prevent content that runs in one zone from gaining the elevated privileges of another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes.

Default Value:

Enabled

8 Security Zones

8.1 Internet Zone

8.1.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Select `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to `High Safety`. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code, sites located in this security zone are more likely to be hosted by malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

Default Value:

High Safety

8.1.2 Set 'Allow paste operations via script' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether scripts can perform a clipboard operation (for example, cut, copy, and paste) in the security zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

A malicious script could use the clipboard in an undesirable manner, for example, if the user had recently copied confidential information to the clipboard while editing a document a malicious script could harvest that information. It might be possible to exploit other vulnerabilities in order to send the harvested data to the attacker.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\1407
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Allow cut, copy or paste
operations from the clipboard via script
```

Then set the `Allow paste operations via script` option to `Disable`.

Impact:

If you enable this policy setting, a script can perform a clipboard operation. If you select Prompt in the drop-down box, users are queried as to whether to perform clipboard

operations. If you disable this policy setting, a script cannot perform a clipboard operation. If you do not configure this policy setting, a script cannot perform a clipboard operation.

Default Value:

Enabled

8.1.3 Set 'Protected Mode' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\2500
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Turn on Protected Mode
```

Then set the `Protected Mode` option to `Enable`.

Impact:

If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode.

8.1.4 Set 'Turn on Cross-Site Scripting (XSS) Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy controls whether or not the Cross-Site Scripting (XSS) Filter will detect and prevent cross-site script injections into websites in this zone. If you enable this policy setting, the XSS Filter is turned on for sites in this zone, and the XSS Filter attempts to block cross-site script injections. If you disable this policy setting, the XSS Filter is turned off for sites in this zone, and Internet Explorer permits cross-site script injections. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

The Cross-Site Scripting (XSS) Filter will detect and prevent cross-site script injections into websites in this zone

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\1409
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Turn on Cross-Site
Scripting Filter
```

Then set the `Turn on Cross-Site Scripting (XSS) Filter` option to `Enable`.

Impact:

If you enable this policy setting, the XSS Filter is turned on for sites in this zone, and the XSS Filter attempts to block cross-site script injections. If you disable this policy setting, the XSS Filter is turned off for sites in this zone, and Internet Explorer permits cross-site script injections.

8.1.5 Set 'Run .NET Framework-reliant components signed with Authenticode' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether .NET Framework components that are signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link. If you enable this policy setting, Internet Explorer will execute signed managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute signed managed components. If you disable this policy setting, Internet Explorer will not execute signed managed components. If you do not configure this policy setting, Internet Explorer will execute signed managed components. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, Internet Explorer will execute signed managed components, it may be possible for someone to host malicious content on a website that takes advantage of these components.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\2001
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Run .NET Framework-reliant components signed with Authenticode
```

Then set the `Run .NET Framework-reliant components signed with Authenticode` option to `Disable`.

Impact:

If you enable this policy setting, Internet Explorer will execute signed managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute signed managed components. If you disable this policy setting, Internet Explorer will not execute signed managed components. If you do not configure this policy setting, Internet Explorer will not execute signed managed components.

8.1.6 Set 'Use Pop-up Blocker' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

Pop-up windows have been used on web sites that host malicious content to trick users into clicking on dangerous links or to confuse users by hiding elements of the browser interface.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1809
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Use Pop-up Blocker
```

Then set the `Use Pop-up Blocker` option to `Enable`.

Impact:

If you enable this policy setting, many unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you do not configure this policy setting, many unwanted pop-up windows are prevented from appearing.

Default Value:

Enabled

8.1.7 Set 'Scriptlets' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether scriptlets can be allowed. If you enable this policy setting, users will be able to run scriptlets. If you disable this policy setting, users will not be able to run scriptlets. If you do not configure this policy setting, a scriptlet can be enabled or disabled by the user. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Scriptlets have been exploited by malicious users in the past, one example is the malware `Exploit-MSWord.k` which embedded the class ID of the Microsoft Scriptlet Component within a Word document and the URL of a website that hosted additional malicious software. When opened Microsoft Word would process the embedded object then download and activate the malicious payload. This particular vulnerability was patched several years ago but disabling this setting in untrusted zones helps mitigate against the entire class of attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1209
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Allow Scriptlets
```

Then set the `Scriptlets` option to `Disable`.

Impact:

If you enable this policy setting, users will be able to run scriptlets. If you disable this policy setting, users will not be able to run scriptlets. If you do not configure this policy setting, a scriptlet can be enabled or disabled by the user.

8.1.8 Set 'Only allow approved domains to use ActiveX controls without prompt' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on websites other than the website that installed the ActiveX control. If you enable this policy setting, the user is prompted before ActiveX controls can run from websites in this zone. The user can choose to allow the control to run from the current site or from all sites. If you disable this policy setting, the user does not see the per-site ActiveX prompt, and ActiveX controls can run from all sites in this zone. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the user were to disable the setting for the zone, malicious ActiveX controls could be executed without the user's knowledge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\120b
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Allow only approved domains to use ActiveX controls without prompt
```

Then set the `Only allow approved domains to use ActiveX controls without prompt` option to `Enable`.

Impact:

Disabling this setting would allow the possibility for malicious ActiveX controls to be executed from non-approved domains within this zone without the user's knowledge.

8.1.9 Set 'Allow drag and drop or copy and paste files' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users can drag files or copy and paste files from a source within the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Content hosted on sites located in the Restricted Sites Zone are more likely to contain malicious payloads and therefor this feature should be blocked for this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\1802
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Allow drag and drop or
copy and paste files
```

Then set the `Allow drag and drop or copy and paste files` option to `Disable`.

Impact:

If you enable this policy setting, users can drag files or copy and paste files from this zone automatically. If you select `Prompt` in the drop-down box, users are queried to choose whether to drag or copy files from this zone. If you disable this policy setting, users are prevented from dragging files or copying and pasting files from this zone.

Default Value:

Enabled

8.1.10 Set 'Run .NET Framework-reliant components not signed with Authenticode' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link. If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will execute unsigned managed components. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Unsigned components may have a greater chance of including malicious code and it is more difficult to determine the author of the application therefore they should be avoided if possible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2004
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Run .NET Framework-reliant components not signed with Authenticode
```

Then set the `Run .NET Framework-reliant components not signed with Authenticode` option to `Disable`.

Impact:

If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will not execute unsigned managed components.

8.1.11 Set 'Internet Explorer web browser control' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether a page can control embedded `WebBrowser` controls via script. If you enable this policy setting, script access to the `WebBrowser` control is allowed. If you disable this policy setting, script access to the `WebBrowser` control is not allowed.

If you do not configure this policy setting, the user can enable or disable script access to the `WebBrowser` control. By default, script access to the `WebBrowser` control is allowed only in the Local Machine and Intranet zones. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

A website hosted by a malicious person could attempt to exploit this feature. For example, in the past there have been cross-site scripting vulnerabilities that were exploited to use various `WebBrowser` controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\1206
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Allow scripting of
Internet Explorer WebBrowser controls
```

Then set the `Internet Explorer web browser control` option to `Disable`.

Impact:

If you enable this policy setting, script access to the `WebBrowser` control is allowed. If you disable this policy setting, script access to the `WebBrowser` control is not allowed. If you do not configure this policy setting, the user can enable or disable script access to the `WebBrowser` control. By default, script access to the `WebBrowser` control is allowed only in the Local Machine and Intranet zones.

8.1.12 Set 'Download unsigned ActiveX controls' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users may download unsigned ActiveX controls from the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Unsigned code is potentially harmful, especially when coming from an untrusted zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1004
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Download unsigned ActiveX controls
```

Then set the `Download unsigned ActiveX controls` option to `Disable`.

Impact:

If you enable this policy setting, users can run unsigned controls without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow the unsigned control to run. If you disable this policy setting, users cannot run unsigned controls. If you do not configure this policy setting, users cannot run unsigned controls.

Default Value:

Disabled

8.1.13 Set 'Download signed ActiveX controls' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Signed code is better than unsigned code in that it may be easier to determine its author, but it is still potentially harmful, especially when coming from an untrusted zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1001
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Download signed ActiveX controls
```

Then set the `Download signed ActiveX controls` option to `Disable`.

Impact:

If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by untrusted publishers. Code signed by trusted publishers is silently downloaded. If you Disable the policy setting, signed controls cannot be downloaded.

Default Value:

Prompt

8.1.14 Set 'Allow font downloads' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether pages of the zone may download HTML fonts. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

It is possible that a font could include malformed data that would cause Internet Explorer to crash when it attempts to load and render the font.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1604
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Allow font downloads
```

Then set the `Allow font downloads` option to `Disable`.

Impact:

If you enable this policy setting, HTML fonts can be downloaded automatically. If you enable this policy setting and Prompt is selected in the drop-down box, users are queried whether to allow HTML fonts to download. If you disable this policy setting, HTML fonts are prevented from downloading.

Default Value:

Enabled

8.1.15 Set 'Launching programs and unsafe files' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not the "Open File - Security Warning" message appears when the user tries to open executable files or other potentially unsafe files (from an intranet file share by using File Explorer, for example). If you enable this policy setting and set the drop-down box to Enable, these files open without a security warning. If you set the drop-down box to Prompt, a security warning appears before the files open. If you disable this policy setting, these files do not open. If you do not configure this policy setting, the user can configure how the computer handles these files. By default, these files are blocked in the Restricted zone, enabled in the Intranet and Local Computer zones, and set to prompt in the Internet and Trusted zones. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

The security warning may help the user to avoid some types of malware hosted on sites run by malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1806
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Show security warning for potentially unsafe files
```

Then set the `Launching programs and unsafe files` option to `Disable`.

Impact:

If you enable this policy setting and set the drop-down box to Enable, these files open without a security warning. If you set the drop-down box to Prompt, a security warning appears before the files open. If you disable this policy setting, these files do not open. If you do not configure this policy setting, the user can configure how the computer handles these files. By default, these files are blocked in the Restricted zone, enabled in the Intranet and Local Computer zones, and set to prompt in the Internet and Trusted zones.

8.1.16 Set 'Automatic prompting for file downloads' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether users will be prompted for non user-initiated file downloads. Regardless of this setting, users will receive file download dialogs for user-initiated downloads. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Users may accept downloads that they did not request, those downloaded files may include malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2200
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Automatic prompting for file downloads
```

Then set the `Automatic prompting for file downloads` option to `Disable`.

Impact:

If you enable this setting, users will receive a file download dialog for automatic download attempts. If you disable or do not configure this setting, file downloads that are not user-initiated will be blocked, and users will see the Information Bar instead of the file download dialog. Users can then click the Information Bar to allow the file download prompt.

Default Value:

Disabled

8.1.17 Set 'Allow installation of desktop items' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users can install Active Desktop items from this zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Active Desktop items could contain links to unauthorized websites or other undesirable content, it is prudent to prevent users from installing desktop items from this security zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1800
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Allow installation of desktop items
```

Then set the `Allow installation of desktop items` option to `Disable`.

Impact:

The settings for this option are: Enabled, users can install desktop items from this zone automatically. Prompt, users are queried to choose whether to install desktop items from this zone. Disabled, users are prevented from installing desktop items from this zone. If you do not configure this policy setting, users are prevented from installing desktop items from this zone.

Default Value:

Prompt

8.1.18 Set 'XAML Files' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the loading of Extensible Application Markup Language (XAML) files. XAML is an XML-based declarative markup language commonly used for creating rich user interfaces and graphics that take advantage of the Windows Presentation Foundation. If you enable this policy setting and set the drop-down box to Enable, XAML files are automatically loaded inside Internet Explorer. The user cannot change this behavior. If you set the drop-down box to Prompt, the user is prompted for loading XAML files. If you disable this policy setting, XAML files are not loaded inside Internet Explorer. The user cannot change this behavior. If you do not configure this policy setting, the user can decide whether to load XAML files inside Internet Explorer. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Enabling loading of XAML files is a risky configuration due to the broad attack surface exposed by the feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\2402
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Allow loading of XAML
files
```

Then set the `XAML Files` option to `Disable`.

Impact:

If you enable this policy setting and set the drop-down box to Enable, XAML files are automatically loaded inside Internet Explorer. The user cannot change this behavior. If you set the drop-down box to Prompt, the user is prompted for loading XAML files. If you disable this policy setting, XAML files are not loaded inside Internet Explorer. The user cannot change this behavior. If you do not configure this policy setting, the user can decide whether to load XAML files inside Internet Explorer.

8.1.19 Set 'Initialize and script ActiveX controls not marked as safe' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage ActiveX controls not marked as safe. If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. This increases the risk of malicious code being loaded and executed by the browser.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1201
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Initialize and script
ActiveX controls not marked as safe
```

Then set the `Initialize and script ActiveX controls not marked as safe` option to `Disable`.

Impact:

If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted.

Default Value:

Disabled

8.1.20 Set 'Enable MIME Sniffing' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage MIME sniffing for file promotion from one type to another based on a MIME sniff. A MIME sniff is the recognition by Internet Explorer of the file type based on a bit signature. If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process. If you do not configure this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

The MIME Sniffing Safety Feature improves security in some scenarios by providing an added layer of defense against potentially malicious files. The feature also helps with compatibility issues caused by web servers that specify incorrect MIME types. Under certain circumstances it can actually increase the risk of compromise because Internet Explorer may detect a script embedded within content that has a non-script MIME type declared and execute the script.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\2100
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Enable MIME Sniffing
```

Then set the `Enable MIME Sniffing` option to `Enable`.

Impact:

If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone; the security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process. If you do not configure this policy setting, the MIME Sniffing Safety Feature will not apply in this zone.

Default Value:

Enabled

8.1.21 Set 'Logon options' to 'Enabled:Prompt for user name and password' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage settings for logon options. If you enable this policy setting, you can choose from the following logon options: Anonymous logon disables HTTP authentication and uses the guest account only for the Common Internet File System (CIFS) protocol. Prompt for user name and password queries users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session. Automatic logon only in Intranet zone queries users for user IDs and passwords in other

zones. After a user is queried, these values can be used silently for the remainder of the session. Automatic logon with current user name and password attempts logon using Windows NT Challenge Response (also known as NTLM authentication). If Windows NT Challenge Response is supported by the server, the logon uses the user's network user name and password for logon. If Windows NT Challenge Response is not supported by the server, the user is queried to provide the user name and password. If you disable this policy setting, logon is set to Automatic logon only in Intranet zone. If you do not configure this policy setting, logon is set to Automatic logon only in Intranet zone. The recommended state for this setting is: `Enabled:Prompt for user name and password`.

Rationale:

Users could submit credentials to servers operated by malicious people who could then attempt to connect to legitimate servers with those captured credentials.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1A00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Logon options
```

Then set the `Logon options` option to `Prompt for user name and password`.

Impact:

Prompt for user name and password queries users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session.

Default Value:

Automatic logon only in Intranet zone

8.1.22 Set 'Access data sources across domains' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Internet Explorer can access data from another security zone using the Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO). The recommended state for this setting is: `Enabled:Disable`.

Rationale:

The ability to access data across domains could cause the user to unknowingly access content hosted on an unauthorized server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1406
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Access data sources across domains
```

Then set the `Access data sources across domains` option to `Disable`.

Impact:

If you enable this policy setting, users can load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you select Prompt in the drop-down box, users are queried to choose whether to allow a page to be loaded in the zone that uses MSXML or ADO to access data from another site in the zone. If you disable this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you do not configure this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone.

Default Value:

Disabled

8.1.23 Set 'Status bar updates via script' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether script is allowed to update the status bar within the zone. If you enable this policy setting, script is allowed to update the status bar. If you disable or do not configure this policy setting, script is not allowed to update the status bar. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

A script running in the zone could cause false information to be displayed on the status bar, which could confuse the user and cause him to perform an undesirable action.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2103
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Allow updates to status bar via script
```

Then set the `Status bar updates via script` option to `Enable`.

Impact:

If you enable this policy setting, script is allowed to update the status bar. If you disable this policy setting, script is not allowed to update the status bar. If you do not configure this policy setting, status bar updates via scripts will be disabled.

8.1.24 Set 'Include local directory path when uploading files to a server' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not local path information is sent when the user is uploading a file via an HTML form. If the local path information is sent, some information may be unintentionally revealed to the server. For instance, files sent from the user's desktop may contain the user name as a part of the path. If you enable this policy setting, path information is sent when the user is uploading a file via an HTML form. If you disable this policy setting, path information is removed when the user is uploading a file via an HTML form. If you do not configure this policy setting, the user can choose whether path information is sent when he or she is uploading a file via an HTML form. By default, path information is sent. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

A site hosted by a malicious user could use this feature to gather information about the file system structure of the user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\160A
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Include local path when user is uploading files to a server
```

Then set the `Include local directory path when uploading files to a server` option to `Disable`.

Impact:

If you enable this policy setting, path information is sent when the user is uploading a file via an HTML form. If you disable this policy setting, path information is removed when the user is uploading a file via an HTML form. If you do not configure this policy setting, the user can choose whether path information is sent when he or she is uploading a file via an HTML form. By default, path information is sent.

8.1.25 Set 'Userdata persistence' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the preservation of information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. When a user returns to a persisted page, the state of the page can be restored if this policy setting is appropriately configured. If you enable this policy setting, users can preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. If you disable this policy setting, users cannot preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. If you do not configure this policy setting, users can preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Organizations may want to disable this feature in order to prevent business data from being stored by Internet Explorer, in the past some sites hosting malicious content exploited this feature as part of an attack against visitors browsing the site.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1606
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Userdata persistence
```

Then set the `Userdata persistence` option to `Disable`.

Impact:

If you enable this policy setting, users can preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. If you disable this policy setting, users cannot preserve information in the browser's history, in favorites, in

an XML store, or directly within a Web page saved to disk. If you do not configure this policy setting, users can preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk.

8.1.26 Set 'Enable dragging of content from different domains within a window' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to set options for dragging content from one domain to a different domain when the source and destination are in the same window. If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy setting or do not configure it, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Content hosted on untrusted sites are more likely to contain malicious payloads and therefor this feature should be blocked for this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\2708
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Enable dragging of content from different domains within a window
```

Then set the `Enable dragging of content from different domains within a window` option to `Disable`.

Impact:

If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy setting or do not configure it, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog.

8.1.27 Set 'Navigate windows and frames across different domains' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the opening of sub-frames and access of applications across different domains. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

It is conceivable that a web site hosting malicious could use this feature to conduct an similar to cross-site scripting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1607
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Navigate windows and frames across different domains
```

Then set the `Navigate windows and frames across different domains` option to `Disable`.

Impact:

If you enable this policy setting, users can open sub-frames from other domains and access applications from other domains. If you select Prompt in the drop-down box, users are queried whether to allow sub-frames or access to applications from other domains. If you disable this policy setting, users cannot open sub-frames or access applications from different domains. If you do not configure this policy setting, users can open sub-frames from other domains and access applications from other domains.

Default Value:

Disabled

8.1.28 Set 'Enable dragging of content from different domains across windows' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to set options for dragging content from one domain to a different domain when the source and destination are in different windows. If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when both the source and destination are in

different windows. Users cannot change this setting. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in different windows. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy or do not configure it, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Content hosted on untrusted sites are more likely to contain malicious payloads and therefor this feature should be blocked for this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2709
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Enable dragging of content from different domains across windows
```

Then set the `Enable dragging of content from different domains across windows` option to `Disable`.

Impact:

If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when both the source and destination are in different windows. Users cannot change this setting. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in different windows. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy or do not configure it, users can drag content

from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting.

8.1.29 Set 'Allow script-initiated windows without size or position constraints' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, scripts will be able to launch and resize additional browser windows without and limits on size or position, attackers have used this feature in the past to confuse users and cause them to click on links that led to undesirable consequences.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2102
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Allow script-initiated windows without size or position constraints
```

Then set the `Allow script-initiated windows without size or position constraints` option to `Disable`.

Impact:

If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you

disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.

Default Value:

Disabled

8.1.30 Set 'Launching applications and files in an IFRAME' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether applications may be run and files may be downloaded from an IFRAME reference in the HTML of the pages in this zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, applications can run and files can be downloaded from IFRAMEs on the pages in this zone without user intervention.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1804
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Launching applications and
files in an IFRAME
```

Then set the `Launching applications and files in an IFRAME` option to `Disable`.

Impact:

If you enable this policy setting, users can run applications and download files from IFRAMEs on the pages in this zone without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to run applications and download files from IFRAMEs on the pages in this zone. If you disable this policy setting, users are prevented from running applications and downloading files from IFRAMEs on the pages in this zone. If you do not configure this policy setting, users are queried to choose whether to run applications and download files from IFRAMEs on the pages in this zone.

Default Value:

Prompt

8.1.31 Set 'Software channel permissions' to 'Enabled:High safety' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage software channel permissions. If you enable this policy setting, you can choose the following options from the drop-down box: The recommended state for this setting is: `Enabled:High safety`.

Rationale:

Any setting lower than High Safety could cause a user to install software that includes malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\100000
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Software channel permissions
```

Then set the `Software channel permissions` option to `High safety`.

Impact:

Low safety allows a user to be notified of software updates by e-mail, software packages to be automatically downloaded to a user's computers, and software packages to be automatically installed on a user's computers. Medium safety allows a user to be notified of software updates by e-mail and software packages to be automatically downloaded to (but not installed on) a user's computers. High safety prevents a user from being notified of software updates by e-mail, and from having software packages automatically downloaded or automatically installed on the user's computers. If you disable this policy setting, permissions are set to High safety.

Default Value:

Medium Safety

8.1.32 Configure 'First-Run Opt-In' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the first-run response that the user sees on a zone-by-zone basis. When the user encounters a new control that has not previously run in Internet Explorer, he or she may be prompted to approve the control. This policy setting determines whether the user is prompted. If you enable this policy setting, the first-run prompt is turned off in the corresponding zone. If you disable this policy setting, the first-run prompt is turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned off by default. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

The first-run prompt may help the user to avoid some types of malware hosted on sites run by malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1208
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Internet Zone\Turn off first-run prompt: First-Run Opt-In
```

Impact:

If you enable this policy setting, the first-run prompt is turned off in the corresponding zone. If you disable this policy setting, the first-run prompt is turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned on by default.

8.1.33 Set 'Web sites in less privileged Web content zones can navigate into this zone' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Web sites from less privileged zones can navigate into this zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\2101
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone\Web sites in less
privileged Web content zones can navigate into this zone
```

Then set the `Web sites in less privileged Web content zones can navigate into this zone` option to `Disable`.

Impact:

If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.

Default Value:

Enabled

8.1.34 Set 'Don't run antimalware programs against ActiveX controls' to 'Enabled:Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer runs antimalware programs against ActiveX controls, to check if they're safe to load on pages.

If you enable this policy setting, Internet Explorer won't check with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you disable this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you don't configure this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control. Users can turn this behavior on or off, using Internet Explorer Security settings.

Rationale:

Scanning ActiveX controls for malware will reduce risk associated with malicious ActiveX controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\3\270C
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:Disabled.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Internet Zone
```

8.2 Intranet Zone

8.2.1 Set 'Java permissions' to 'Enabled:High safety' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Select `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. Disable Java to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to `Medium Safety`. The recommended state for this setting is: `Enabled:High safety`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Intranet Zone\Java permissions
```

Then set the `Java permissions` option to `High safety`.

8.2.2 Set 'Initialize and script ActiveX controls not marked as safe' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage ActiveX controls not marked as safe. If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. This increases the risk of malicious code being loaded and executed by the browser.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\1201
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Intranet Zone\Initialize and script ActiveX controls not marked as safe
```

Then set the `Initialize and script ActiveX controls not marked as safe` option to `Disable`.

Impact:

If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted.

Default Value:

Disabled

8.2.3 Set 'Intranet Sites: Include all network paths (UNCs)' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether URLs representing UNCs are mapped into the local Intranet security zone. The recommended state for this setting is: `Disabled`.

Rationale:

Some UNC paths could refer to servers not managed by the organization which means they could host malicious content and therefor it is safest to not include all UNC paths in the Intranet Sites zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Intranet Sites: Include all network paths (UNCs)
```

Impact:

If you enable this policy setting, all network paths are mapped into the Intranet Zone. If you disable this policy setting, network paths are not necessarily mapped into the Intranet Zone (other rules might map one there).
If you do not configure this policy setting, users choose whether network paths are mapped into the Intranet Zone.

Default Value:

Not configured.

8.2.4 Set 'Don't run antimalware programs against ActiveX controls' to 'Enabled:Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer runs antimalware programs against ActiveX controls, to check if they're safe to load on pages.

If you enable this policy setting, Internet Explorer won't check with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you disable this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you don't configure this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control. Users can turn this behavior on or off, using Internet Explorer Security settings.

Rationale:

Scanning ActiveX controls for malware will reduce risk associated with malicious ActiveX controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\1\270C
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:Disabled.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Intranet Zone
```

8.3 Restricted Sites Zone

8.3.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set to `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to `High Safety`. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code, sites located in this security zone are more likely to be hosted by malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

Default Value:

High Safety

8.3.2 Set 'Allow drag and drop or copy and paste files' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users can drag files or copy and paste files from a source within the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Content hosted on sites located in the Restricted Sites Zone are more likely to contain malicious payloads and therefor this feature should be blocked for this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1802
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow drag and drop or copy and paste files
```

Then set the `Allow drag and drop or copy and paste files` option to `Disable`.

Impact:

If you enable this policy setting, users can drag files or copy and paste files from this zone automatically. If you select Prompt in the drop-down box, users are queried to choose whether to drag or copy files from this zone. If you disable this policy setting, users are prevented from dragging files or copying and pasting files from this zone.

Default Value:

Disabled

8.3.3 Set 'Download signed ActiveX controls' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Signed code is better than unsigned code in that it may be easier to determine its author, but it is still potentially harmful, especially when coming from an untrusted zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1001
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Download signed ActiveX controls
```

Then set the `Download signed ActiveX controls` option to `Disable`.

Impact:

If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by untrusted publishers. Code signed by trusted publishers is silently downloaded. If you Disable the policy setting, signed controls cannot be downloaded.

Default Value:

Disabled

8.3.4 Set 'Script ActiveX controls marked safe for scripting' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether an ActiveX control marked safe for scripting can interact with a script. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, script interaction can occur automatically without user intervention.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1405
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Script ActiveX controls marked safe for scripting
```

Then set the `Script ActiveX controls marked safe for scripting` option to `Disable`.

Impact:

If you enable this policy setting, script interaction can occur automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow script interaction. If you disable this policy setting or do not configure this policy setting, script interaction is prevented from occurring.

Default Value:

Disabled

8.3.5 Set 'Allow active scripting' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether script code on pages in the zone is run. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Active scripts hosted on sites located in this zone are more likely to contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1400
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow active scripting
```

Then set the `Allow active scripting` option to `Disable`.

Impact:

If you enable this policy setting, script code on pages in the zone can run automatically. If you select Prompt in the drop-down box, users are queried to choose whether to allow script code on pages in the zone to run. If you disable this policy setting, script code on pages in the zone is prevented from running. If you do not configure this policy setting, script code on pages in the zone is prevented from running.

Default Value:

Disabled

8.3.6 Set 'Turn on Cross-Site Scripting (XSS) Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy controls whether or not the Cross-Site Scripting (XSS) Filter will detect and prevent cross-site script injections into websites in this zone. If you enable this policy setting, the XSS Filter is turned on for sites in this zone, and the XSS Filter attempts to block cross-site script injections. If you disable this policy setting, the XSS Filter is turned off for sites in this zone, and Internet Explorer permits cross-site script injections. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

The Cross-Site Scripting (XSS) Filter will detect and prevent cross-site script injections into websites in this zone

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1409
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Turn on Cross-Site Scripting Filter
```

Then set the `Turn on Cross-Site Scripting (XSS) Filter` option to `Enable`.

8.3.7 Set 'Initialize and script ActiveX controls not marked as safe' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage ActiveX controls not marked as safe. If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. This increases the risk of malicious code being loaded and executed by the browser.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1201
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Initialize and script ActiveX controls not marked as safe
```

Then set the `Initialize and script ActiveX controls not marked as safe` option to `Disable`.

Impact:

If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted.

Default Value:

Disabled

8.3.8 Set 'Run .NET Framework-reliant components signed with Authenticode' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether .NET Framework components that are signed with Authenticode can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, Internet Explorer will execute signed managed components, it may be possible for someone to host malicious content on a website that takes advantage of these components.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2001
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Run .NET
Framework-reliant components signed with Authenticode
```

Then set the `Run .NET Framework-reliant components signed with Authenticode` option to `Disable`.

Impact:

If you enable this policy setting, Internet Explorer will execute signed managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute signed managed components. If you disable this policy setting, Internet Explorer will not execute signed managed components. If you do

not configure this policy setting, Internet Explorer will not execute signed managed components.

Default Value:

Disabled

8.3.9 Set 'Allow paste operations via script' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether scripts can perform a clipboard operation (for example, cut, copy, and paste) in the security zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

A malicious script could use the clipboard in an undesirable manner, for example, if the user had recently copied confidential information to the clipboard while editing a document a malicious script could harvest that information. It might be possible to exploit other vulnerabilities in order to send the harvested data to the attacker.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1407
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow cut, copy or paste operations from the clipboard via script
```

Then set the `Allow paste operations via script` option to `Disable`.

Impact:

If you enable this policy setting, a script can perform a clipboard operation. If you select Prompt in the drop-down box, users are queried as to whether to perform clipboard operations. If you disable this policy setting, a script cannot perform a clipboard operation. If you do not configure this policy setting, a script cannot perform a clipboard operation.

Default Value:

Disabled

8.3.10 Set 'Protected Mode' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode will be turned on. Users will not be able to turn off protected mode. If you disable this policy setting, Protected Mode will be turned off. It will revert to Internet Explorer 6 behavior that allows for Internet Explorer to write to the registry and the file system. Users will not be able to turn on protected mode. If you do not configure this policy, users will be able to turn on or off protected mode. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

Protected mode protects Internet Explorer from exploited vulnerabilities by reducing the locations Internet Explorer can write to in the registry and the file system.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2500
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Turn on Protected Mode
```

Then set the `Protected Mode` option to `Enable`.

8.3.11 Set 'Allow installation of desktop items' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users can install Active Desktop items from this zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Active Desktop items could contain links to unauthorized websites or other undesirable content, it is prudent to prevent users from installing desktop items from this security zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1800
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow installation of desktop items
```

Then set the `Allow installation of desktop items` option to `Disable`.

Impact:

The settings for this option are: Enabled, users can install desktop items from this zone automatically. Prompt, users are queried to choose whether to install desktop items from this zone. Disabled, users are prevented from installing desktop items from this zone. If you

do not configure this policy setting, users are prevented from installing desktop items from this zone.

Default Value:

Disabled

8.3.12 Set 'Launching programs and unsafe files' to 'Enabled:Prompt' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not the "Open File - Security Warning" message appears when the user tries to open executable files or other potentially unsafe files (from an intranet file share by using File Explorer, for example). If you enable this policy setting and set the drop-down box to Enable, these files open without a security warning. If you set the drop-down box to Prompt, a security warning appears before the files open. If you disable this policy setting, these files do not open. If you do not configure this policy setting, the user can configure how the computer handles these files. By default, these files are blocked in the Restricted zone, enabled in the Intranet and Local Computer zones, and set to prompt in the Internet and Trusted zones. The recommended state for this setting is: `Enabled:Prompt`.

Rationale:

The security warning may help the user to avoid some types of malware hosted on sites run by malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1806
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Show security
warning for potentially unsafe files
```

Then set the `Launching programs and unsafe files` option to `Prompt`.

8.3.13 Set 'Automatic prompting for file downloads' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether users will be prompted for non user-initiated file downloads. Regardless of this setting, users will receive file download dialogs for user-initiated downloads. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Users may accept downloads that they did not request, those downloaded files may include malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2200
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Automatic
prompting for file downloads
```

Then set the `Automatic prompting for file downloads` option to `Disable`.

Impact:

If you enable this setting, users will receive a file download dialog for automatic download attempts. If you disable or do not configure this setting, file downloads that are not user-initiated will be blocked, and users will see the Information Bar instead of the file

download dialog. Users can then click the Information Bar to allow the file download prompt.

Default Value:

Disabled

8.3.14 Set 'XAML Files' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the loading of Extensible Application Markup Language (XAML) files. XAML is an XML-based declarative markup language commonly used for creating rich user interfaces and graphics that take advantage of the Windows Presentation Foundation. If you enable this policy setting and set the drop-down box to Enable, XAML files are automatically loaded inside Internet Explorer. The user cannot change this behavior. If you set the drop-down box to Prompt, the user is prompted for loading XAML files. If you disable this policy setting, XAML files are not loaded inside Internet Explorer. The user cannot change this behavior. If you do not configure this policy setting, the user can decide whether to load XAML files inside Internet Explorer. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Enabling loading of XAML files is a risky configuration due to the broad attack surface exposed by the feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\2402
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow loading of
XAML files
```

Then set the `XAML Files` option to `Disable`.

8.3.15 Set 'Allow font downloads' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether pages of the zone may download HTML fonts. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

It is possible that a font could include malformed data that would cause Internet Explorer to crash when it attempts to load and render the font.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\1604
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow font
downloads
```

Then set the `Allow font downloads` option to `Disable`.

Impact:

If you enable this policy setting, HTML fonts can be downloaded automatically. If you enable this policy setting and Prompt is selected in the drop-down box, users are queried whether to allow HTML fonts to download. If you disable this policy setting, HTML fonts are prevented from downloading.

Default Value:

Disabled

8.3.16 Set 'Enable MIME Sniffing' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage MIME sniffing for file promotion from one type to another based on a MIME sniff. A MIME sniff is the recognition by Internet Explorer of the file type based on a bit signature. If you enable this policy setting, the MIME Sniffing Safety Feature will not apply in this zone. The security zone will run without the added layer of security provided by this feature. If you disable this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process. If you do not configure this policy setting, the actions that may be harmful cannot run; this Internet Explorer security feature will be turned on in this zone, as dictated by the feature control setting for the process. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

The MIME Sniffing Safety Feature improves security in some scenarios by providing an added layer of defense against potentially malicious files. The feature also helps with compatibility issues caused by web servers that specify incorrect MIME types. Under certain circumstances it can actually increase the risk of compromise because Internet Explorer may detect a script embedded within content that has a non-script MIME type declared and execute the script.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2100
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Enable MIME
Sniffing
```

Then set the `Enable MIME Sniffing` option to `Enable`.

Default Value:

Enabled

8.3.17 Set 'Internet Explorer web browser control' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether a page can control embedded `WebBrowser` controls via script. If you enable this policy setting, script access to the `WebBrowser` control is allowed. If you disable this policy setting, script access to the `WebBrowser` control is not allowed. If you do not configure this policy setting, the user can enable or disable script access to the `WebBrowser` control. By default, script access to the `WebBrowser` control is allowed only in the Local Machine and Intranet zones. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

A website hosted by a malicious person could attempt to exploit this feature. For example, in the past there have been cross-site scripting vulnerabilities that were exploited to use various `WebBrowser` controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\1206
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow scripting of
Internet Explorer WebBrowser controls
```

Then set the `Internet Explorer web browser control` option to `Disable`.

8.3.18 Set 'Allow Binary and Script Behaviors' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage dynamic binary and script behaviors: components that encapsulate specific functionality for HTML elements to which they were attached. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Executable binaries and scripts may include malicious code, the risk of this is higher in the Restricted Sites Zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2000
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow binary and
script behaviors
```

Then set the `Allow Binary and Script Behaviors` option to `Disable`.

Impact:

If you enable this policy setting, binary and script behaviors are available. If you select Administrator approved in the drop-down box, only behaviors listed in the Admin-approved Behaviors under Binary Behaviors Security Restriction policy are available. If you

disable this policy setting, binary and script behaviors are not available unless applications have implemented a custom security manager. If you do not configure this policy setting, binary and script behaviors are not available unless applications have implemented a custom security manager.

Default Value:

Disabled

8.3.19 Set 'Scripting of Java applets' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether applets are exposed to scripts within the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, scripts can access applets automatically without user intervention.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1402
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Scripting of Java applets
```

Then set the `Scripting of Java applets` option to `Disable`.

Impact:

If you enable this policy setting, scripts can access applets automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow scripts to access applets. If you disable this policy setting or do not configure this policy setting, scripts are prevented from accessing applets.

Default Value:

Disabled

8.3.20 Set 'Use Pop-up Blocker' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether unwanted pop-up windows appear. Pop-up windows that are opened when the end user clicks a link are not blocked. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

Pop-up windows have been used on web sites that host malicious content to trick users into clicking on dangerous links or to confuse users by hiding elements of the browser interface.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1809
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Use Pop-up Blocker
```

Then set the `Use Pop-up Blocker` option to `Enable`.

Impact:

If you enable this policy setting, many unwanted pop-up windows are prevented from appearing. If you disable this policy setting, pop-up windows are not prevented from appearing. If you do not configure this policy setting, many unwanted pop-up windows are prevented from appearing.

Default Value:

Enabled

8.3.21 Set 'Download unsigned ActiveX controls' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether users may download unsigned ActiveX controls from the zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Unsigned code is potentially harmful, especially when coming from an untrusted zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1004
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Download unsigned ActiveX controls
```

Then set the `Download unsigned ActiveX controls` option to `Disable`.

Impact:

If you enable this policy setting, users can run unsigned controls without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow the unsigned control to run. If you disable this policy setting, users cannot run unsigned controls. If you do not configure this policy setting, users cannot run unsigned controls.

Default Value:

Disabled

8.3.22 Set 'Scriptlets' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether scriptlets can be allowed. If you enable this policy setting, users will be able to run scriptlets. If you disable this policy setting, users will not be able to run scriptlets. If you do not configure this policy setting, a scriptlet can be enabled or disabled by the user. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Scriptlets have been exploited by malicious users in the past, one example is the malware Exploit-MSWord.k which embedded the class ID of the Microsoft Scriptlet Component within a Word document and the URL of a website that hosted additional malicious software. When opened Microsoft Word would process the embedded object then download and activate the malicious payload. This particular vulnerability was patched several years ago but disabling this setting in untrusted zones helps mitigate against the entire class of attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\1209
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow Scriptlets
```

Then set the `Scriptlets` option to `Disable`.

8.3.23 Set 'Allow file downloads' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether file downloads are permitted from the zone. This option is determined by the zone of the page with the link causing the download, not the zone from which the file is delivered. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Sites located in the Restricted Sites Zone are more likely to contain malicious payloads and therefor downloads from this zone should be blocked.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1803
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow file downloads
```

Then set the `Allow file downloads` option to `Disable`.

Impact:

If you enable this policy setting, files can be downloaded from the zone. If you disable this policy setting, files are prevented from being downloaded from the zone. If you do not configure this policy setting, files are prevented from being downloaded from the zone.

Default Value:

Disabled

8.3.24 Set 'Only allow approved domains to use ActiveX controls without prompt' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on websites other than the website that installed the ActiveX control. If you enable this policy setting, the user is prompted before ActiveX controls can run from websites in this zone. The user can choose to allow the control to run from the current site or from all sites. If you disable this policy setting, the user does not see the per-site ActiveX prompt, and ActiveX controls can run from all sites in this zone. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the user were to disable the setting for the zone, malicious ActiveX controls could be executed without the user's knowledge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\120b
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow only
approved domains to use ActiveX controls without prompt
```

Then set the `Only allow approved domains to use ActiveX controls without prompt` option to `Enable`.

Impact:

Disabling this setting would allow the possibility for malicious ActiveX controls to be executed from non-approved domains within this zone without the user's knowledge.

8.3.25 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Turn on
SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.3.26 Set 'Run ActiveX controls and plugins' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether ActiveX controls and plug-ins can be run on pages from the specified zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, controls and plug-ins can run without user intervention.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\1200
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Run ActiveX
controls and plugins
```

Then set the `Run ActiveX controls and plugins` option to `Disable`.

Impact:

If you enable this policy setting, controls and plug-ins can run without user intervention. If you selected Prompt in the drop-down box, users are asked to choose whether to allow the controls or plug-in to run. If you disable this policy setting, controls and plug-ins are prevented from running. If you do not configure this policy setting, controls, and plug-ins are prevented from running.

Default Value:

Disabled

8.3.27 Set 'Run .NET Framework-reliant components not signed with Authenticode' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether .NET Framework components that are not signed with Authenticode® can be executed from Internet Explorer. These components include managed controls referenced from an object tag and managed executables referenced from a link. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Unsigned components may have a greater chance of including malicious code and it is more difficult to determine the author of the application therefore they should be avoided if possible.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\2004
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Run .NET
Framework-reliant components not signed with Authenticode
```

Then set the `Run .NET Framework-reliant components not signed with Authenticode` option to `Disable`.

Impact:

If you enable this policy setting, Internet Explorer will execute unsigned managed components. If you select Prompt in the drop-down box, Internet Explorer will prompt the user to determine whether to execute unsigned managed components. If you disable this policy setting, Internet Explorer will not execute unsigned managed components. If you do not configure this policy setting, Internet Explorer will not execute unsigned managed components.

Default Value:

Disabled

8.3.28 Set 'Logon options' to 'Enabled:Anonymous logon' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage settings for logon options. If you enable this policy setting, you can choose from the following logon options: Anonymous logon disables HTTP authentication and uses the guest account only for the Common Internet File System (CIFS) protocol. Prompt for user name and password queries users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session. Automatic logon only in Intranet zone queries users for user IDs and passwords in other zones. After a user is queried, these values can be used silently for the remainder of the session. Automatic logon with current user name and password attempts logon using Windows NT Challenge Response (also known as NTLM authentication). If Windows NT Challenge Response is supported by the server, the logon uses the user's network user name and password for logon. If Windows NT Challenge Response is not supported by the server, the user is queried to provide the user name and password. If you disable this policy setting, logon is set to Automatic logon only in Intranet zone. If you do not configure this policy setting, logon is set to Automatic logon only in Intranet zone. The recommended state for this setting is: `Enabled:Anonymous logon`.

Rationale:

Users could submit credentials to servers operated by malicious people who could then attempt to connect to legitimate servers with those captured credentials.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1A00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Logon options
```

Then set the `Logon options` option to `Anonymous logon`.

Impact:

Anonymous logon disables HTTP authentication and uses the guest account, which means that users will be unable to connect to sites in this security zone that require authentication.

Default Value:

Prompt for user name and password

8.3.29 Set 'Allow script-initiated windows without size or position constraints' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, scripts will be able to launch and resize additional browser windows without and limits on size or position, attackers have used this feature in the past to confuse users and cause them to click on links that led to undesirable consequences.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\2102
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow script-initiated windows without size or position constraints
```

Then set the `Allow script-initiated windows without size or position constraints` option to `Disable`.

Impact:

If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.

Default Value:

Disabled

8.3.30 Set 'Allow META REFRESH' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether a user's browser can be redirected to another Web page if the author of the Web page uses the Meta Refresh setting to redirect browsers to another Web page. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

It is possible that users will unknowingly be redirected to a site hosting malicious content.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1608
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow META REFRESH
```

Then set the `Allow META REFRESH` option to `Disable`.

Impact:

If you enable this policy setting, a user's browser that loads a page containing an active Meta Refresh setting can be redirected to another Web page. If you disable this policy setting, a user's browser that loads a page containing an active Meta Refresh setting cannot be redirected to another Web page. If you do not configure this policy setting, a user's browser that loads a page containing an active Meta Refresh setting cannot be redirected to another Web page.

Default Value:

Disabled

8.3.31 Set 'Userdata persistence' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the preservation of information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. When a user returns to a persisted page, the state of the page can be restored if this policy setting is appropriately configured. If you enable this policy setting, users can preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. If you disable this policy setting, users cannot preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. If you do not configure this policy setting, users cannot preserve information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Organizations may want to disable this feature in order to prevent business data from being stored by Internet Explorer, in the past some sites hosting malicious content exploited this feature as part of an attack against visitors browsing the site.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1606
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Userdata persistence
```

Then set the `Userdata persistence` option to `Disable`.

8.3.32 Set 'Navigate windows and frames across different domains' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the opening of sub-frames and access of applications across different domains. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

It is conceivable that a web site hosting malicious could use this feature to conduct an similar to cross-site scripting.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1607
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Navigate windows and frames across different domains
```

Then set the `Navigate windows and frames across different domains` option to `Disable`.

Impact:

If you enable this policy setting, users can open sub-frames from other domains and access applications from other domains. If you select Prompt in the drop-down box, users are queried whether to allow sub-frames or access to applications from other domains. If you disable this policy setting, users cannot open sub-frames or access applications from different domains. If you do not configure this policy setting, users can open sub-frames from other domains and access applications from other domains.

Default Value:

Disabled

8.3.33 Set 'Software channel permissions' to 'Enabled:High safety' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage software channel permissions. If you enable this policy setting, you can choose the following options from the drop-down box: Low safety allows a user to be notified of software updates by e-mail, software packages to be automatically downloaded to a user's computers, and software packages to be automatically installed on a user's computers. Medium safety allows a user to be notified of software updates by e-mail and software packages to be automatically downloaded to (but not installed on) a user's computers. High safety prevents a user from being notified of software updates by e-mail, and from having software packages automatically downloaded or automatically installed on the user's computers. If you disable this policy setting, permissions are set to High safety. The recommended state for this setting is: `Enabled:High safety`.

Rationale:

Any setting lower than High Safety could cause a user to install software that includes malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\100000
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Software channel permissions
```

Then set the `Software channel permissions` option to `High safety`.

Impact:

There should be no impact since the recommended setting is also the default.

Default Value:

High safety

8.3.34 Set 'Include local directory path when uploading files to a server' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not local path information is sent when the user is uploading a file via an HTML form. If the local path information is sent, some information may be unintentionally revealed to the server. For instance, files sent from the user's desktop may contain the user name as a part of the path. If you enable this policy setting, path information is sent when the user is uploading a file via an HTML form. If you disable this policy setting, path information is removed when the user is uploading a file via an HTML form. If you do not configure this policy setting, the user can choose whether path information is sent when he or she is uploading a file via an HTML form. By default, path information is sent. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

A site hosted by a malicious user could use this feature to gather information about the file system structure of the user's computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\160A
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Include local path when user is uploading files to a server
```

Then set the `Include local directory path when uploading files to a server` option to `Disable`.

8.3.35 Set 'Enable dragging of content from different domains within a window' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to set options for dragging content from one domain to a different domain when the source and destination are in the same window. If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy setting or do not configure it, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Content hosted on untrusted sites are more likely to contain malicious payloads and therefor this feature should be blocked for this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\2708
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Enable dragging of content from different domains within a window
```

Then set the `Enable dragging of content from different domains within a window` option to `Disable`.

8.3.36 Set 'Status bar updates via script' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether script is allowed to update the status bar within the zone. If you enable this policy setting, script is allowed to update the status bar. If you disable or do not configure this policy setting, script is not allowed to update the status bar. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

A script running in the zone could cause false information to be displayed on the status bar, which could confuse the user and cause him to perform an undesirable action.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\2103
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Allow updates to status bar via script
```

Then set the `Status bar updates via script` option to `Enable`.

Impact:

If you enable this policy setting, script is allowed to update the status bar. If you disable this policy setting, script is not allowed to update the status bar. If you do not configure this policy setting, status bar updates via scripts will be disabled.

8.3.37 Set 'Access data sources across domains' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Internet Explorer can access data from another security zone using the Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO). The recommended state for this setting is: `Enabled:Disable`.

Rationale:

The ability to access data across domains could cause the user to unknowingly access content hosted on an unauthorized server.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\1406
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Access data
sources across domains
```

Then set the `Access data sources across domains` option to `Disable`.

Impact:

If you enable this policy setting, users can load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you select Prompt in the drop-down box, users are queried to choose whether to allow a page to be loaded in the zone that uses MSXML or ADO to access data from another site in the zone. If you disable this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you do not configure this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone.

Default Value:

Disabled

8.3.38 Set 'Web sites in less privileged Web content zones can navigate into this zone' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether Web sites from less privileged zones can navigate into this zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\2101
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Web sites in less privileged Web content zones can navigate into this zone
```

Then set the `Web sites in less privileged Web content zones can navigate into this zone` option to `Disable`.

Impact:

If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you

select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.

Default Value:

Disabled

8.3.39 Configure 'First-Run Opt-In' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the first-run response that the user sees on a zone-by-zone basis. When the user encounters a new control that has not previously run in Internet Explorer, he or she may be prompted to approve the control. This policy setting determines whether the user is prompted. If you enable this policy setting, the first-run prompt is turned off in the corresponding zone. If you disable this policy setting, the first-run prompt is turned on in the corresponding zone. If you do not configure this policy setting, the first-run prompt is turned off by default. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

The first-run prompt may help the user to avoid some types of malware hosted on sites run by malicious people.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\1208
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Turn off first-run prompt: First-Run Opt-In
```

8.3.40 Set 'Enable dragging of content from different domains across windows' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to set options for dragging content from one domain to a different domain when the source and destination are in different windows. If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when both the source and destination are in different windows. Users cannot change this setting. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in different windows. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy or do not configure it, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

Content hosted on untrusted sites are more likely to contain malicious payloads and therefor this feature should be blocked for this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\2709
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Enable dragging of content from different domains across windows
```

Then set the `Enable dragging of content from different domains across windows` option to `Disable`.

8.3.41 Set 'Launching applications and files in an IFRAME' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage whether applications may be run and files may be downloaded from an IFRAME reference in the HTML of the pages in this zone. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

If you enable this policy setting, applications can run and files can be downloaded from IFRAMEs on the pages in this zone without user intervention.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1804
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone\Launching applications and files in an IFRAME
```

Then set the `Launching applications and files in an IFRAME` option to `Disable`.

Impact:

If you enable this policy setting, users can run applications and download files from IFRAMEs on the pages in this zone without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to run applications and download files from IFRAMEs on the pages in this zone. If you disable this policy setting, users are prevented from running applications and downloading files from IFRAMEs on the pages in this zone. If you do not configure this policy setting, users are queried to choose whether to run applications and download files from IFRAMEs on the pages in this zone.

Default Value:

Disabled

8.3.42 Set 'Don't run antimalware programs against ActiveX controls' to 'Enabled:Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer runs antimalware programs against ActiveX controls, to check if they're safe to load on pages.

If you enable this policy setting, Internet Explorer won't check with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you disable this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you don't configure this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control. Users can turn this behavior on or off, using Internet Explorer Security settings.

Rationale:

Scanning ActiveX controls for malware will reduce risk associated with malicious ActiveX controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\4\270C
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:Disabled.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Restricted Sites Zone
```

8.4 Local Machine Zone

8.4.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set this to `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. Disable Java to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to `Medium Safety`. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Local Machine Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

8.4.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Local Machine Zone\Turn on SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.4.3 Set 'Don't run antimalware programs against ActiveX controls' to 'Enabled:Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer runs antimalware programs against ActiveX controls, to check if they're safe to load on pages.

If you enable this policy setting, Internet Explorer won't check with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you disable this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you don't configure this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control. Users can turn this behavior on or off, using Internet Explorer Security settings.

Rationale:

Scanning ActiveX controls for malware will reduce risk associated with malicious ActiveX controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\0\270C
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:Disabled.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Local Machine Zone
```

8.5 Trusted Sites Zone

8.5.1 Set 'Java permissions' to 'Enabled:High safety' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set to `Custom` to control permissions settings individually. `Low Safet`y enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, the permission is set to `Low Safety`. The recommended state for this setting is: `Enabled:High safety`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Trusted Sites Zone\Java permissions
```

Then set the `Java permissions` option to `High safety`.

8.5.2 Set 'Initialize and script ActiveX controls not marked as safe' to 'Enabled:Disable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage ActiveX controls not marked as safe.

If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option.

If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted.

If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted.

If you do not configure this policy setting, users are queried whether to allow the control to be loaded with parameters or scripted. The recommended state for this setting is: `Enabled:Disable`.

Rationale:

This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. This increases the risk of malicious code being loaded and executed by the browser.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Zones\2\1201
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Trusted Sites Zone\Initialize and script ActiveX controls not marked as safe
```

Then set the `Initialize and script ActiveX controls not marked as safe` option to `Disable`.

Default Value:

Prompt

8.5.3 Set 'Don't run antimalware programs against ActiveX controls' to 'Enabled:Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer runs antimalware programs against ActiveX controls, to check if they're safe to load on pages.

If you enable this policy setting, Internet Explorer won't check with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you disable this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control.

If you don't configure this policy setting, Internet Explorer always checks with your anti-malware program to see if it's safe to create an instance of the ActiveX control. Users can turn this behavior on or off, using Internet Explorer Security settings.

Rationale:

Scanning ActiveX controls for malware will reduce risk associated with malicious ActiveX controls.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\270C
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled:Disabled.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Trusted Sites Zone
```

8.6 Locked-Down Internet Zone

8.6.1 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Internet Zone\Turn on SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.6.2 Set 'Only allow approved domains to use ActiveX controls without prompt' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on websites other than the website that installed the ActiveX control. If you enable this policy setting, the user is prompted before ActiveX controls can run from websites in this zone. The user can choose to allow the control to run from the current site or from all sites. If you disable this policy setting, the user does not see the per-site ActiveX prompt, and ActiveX controls can run from all sites in this zone. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the user were to disable the setting for the zone, malicious ActiveX controls could be executed without the user's knowledge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\3\120b
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Internet Zone\Allow only approved domains to use ActiveX controls without prompt
```

Then set the `Only allow approved domains to use ActiveX controls without prompt` option to `Enable`.

Impact:

Disabling this setting would allow the possibility for malicious ActiveX controls to be executed from non-approved domains within this zone without the user's knowledge.

8.7 Locked-Down Intranet Zone

8.7.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set to `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, Java applets are disabled. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Intranet Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

8.7.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\1\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Intranet Zone\Turn on SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.8 Locked-Down Restricted Sites Zone

8.8.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set to `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, Java applets are disabled. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Restricted Sites Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

8.8.2 Set 'Only allow approved domains to use ActiveX controls without prompt' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on websites other than the website that installed the ActiveX control. If you enable this policy setting, the user is prompted before ActiveX controls can run from websites in this zone. The user can choose to allow the control to run from the current site or from all sites. If you disable this policy setting, the user does not see the per-site ActiveX prompt, and ActiveX controls can run from all sites in this zone. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the user were to disable the setting for the zone, malicious ActiveX controls could be executed without the user's knowledge.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\4\120b
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Restricted Sites Zone\Allow only approved domains to use ActiveX controls without prompt
```

Then set the `Only allow approved domains to use ActiveX controls without prompt` option to `Enable`.

Impact:

Disabling this setting would allow the possibility for malicious ActiveX controls to be executed from non-approved domains within this zone without the user's knowledge.

8.8.3 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Lockdown_Zones\4\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Security Page\Locked-Down Restricted Sites Zone\Turn
on SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.9 Locked-Down Local Machine Zone

8.9.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set to `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, Java applets are disabled. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Local Machine Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

8.9.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\0\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Local Machine Zone\Turn on SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.10 Locked-Down Trusted Sites Zone

8.10.1 Set 'Java permissions' to 'Enabled:Disable Java' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Set to `Custom` to control permissions settings individually. `Low Safety` enables applets to perform all operations. `Medium Safety` enables applets to run in their sandbox (an area in memory outside of which the program cannot make calls), plus capabilities like scratch space (a safe and secure storage area on the client computer) and user-controlled file I/O. `High Safety` enables applets to run in their sandbox. `Disable Java` to prevent any applets from running. If you disable this policy setting, Java applets cannot run. If you do not configure this policy setting, Java applets are disabled. The recommended state for this setting is: `Enabled:Disable Java`.

Rationale:

Java applications could contain malicious code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2\1C00
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Trusted Sites Zone\Java permissions
```

Then set the `Java permissions` option to `Disable Java`.

8.10.2 Set 'Use SmartScreen Filter' to 'Enabled:Enable' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content.

If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content.

If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content.

If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content.

Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content. The recommended state for this setting is: `Enabled:Enable`.

Rationale:

If the SmartScreen Filter is enabled globally, not enabling this setting would allow the user to disable the use of the SmartScreen Filter in this zone.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones\2\2301
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Trusted Sites Zone\Turn on SmartScreen Filter scan
```

Then set the `Use SmartScreen Filter` option to `Enable`.

Impact:

The SmartScreen Filter will be used in this zone.

8.11 Set 'Security Zones: Do not allow users to change policies' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

If you enable this policy setting, you disable the Custom Level button and Security level for this zone slider on the Security tab in the Internet Options dialog box. If this policy setting is disabled or not configured, users will be able to change the settings for security zones. It prevents users from changing security zone policy settings that are established by the administrator.

Note: If you enable the `Disable the Security page` setting (located in `\User Configuration\ Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel`) the Security tab is removed from Internet Explorer in Control Panel and the Disable setting takes precedence over this Security Zones: setting. The recommended state for this setting is: `Enabled`.

Rationale:

Users who change their Internet Explorer security settings could enable the execution of dangerous types of code from the Internet and Web sites that were listed in the Restricted Sites zone in the browser.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_options_edit
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Zones: Do not allow users to change policies
```

Default Value:

Disabled

8.12 Set 'Security Zones: Do not allow users to add/delete sites' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

Enable this policy setting to disable the site management settings for security zones. (To see the site management settings for security zones, open Internet Explorer, select Tools and then Internet Options, click the Security tab, and then click Sites.) If this policy setting is disabled or not configured, users will be able to add or remove Web sites in the Trusted Sites and Restricted Sites zones, as well as alter settings in the Local Intranet zone.

Note: If you enable the `Disable the Security page` setting (located in `\User Configuration\ Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel`), the Security tab is removed from the interface and the Disable setting takes precedence over this Security Zones: setting. The recommended state for this setting is: `Enabled`.

Rationale:

If you do not configure this policy setting, users will be able to add or remove sites from the Trusted Sites and Restricted Sites zones at will and change settings in the Local Intranet zone. This configuration could allow sites that host malicious mobile code to be added to these zones, which users could execute.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Security_zones_map_edit
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Zones: Do not allow users to add/delete sites
```

Impact:

Users will not be able to change site management settings for security zones that have been established by the administrator. When users need to add or remove sites from these Internet Explorer security zones, an administrator will have to configure them. Intranet zone. This may impact some business applications if users access them using a URL that appears to be from the Internet. For example, in order to utilize all of the capabilities of Infopath Internet Explorer needs to run the content in the Intranet or Trusted Sites zone. However, if URL provided is an IP address or a fully qualified domain name IE will instead run it in the Internet zone. You can overcome issues such as this by adding the URLs to the Trusted Sites zone.

Default Value:

Disabled

8.13 Set 'Security Zones: Use only machine settings' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting affects how security zone changes apply to different users. If you enable this policy setting, changes that one user makes to a security zone will apply to all users of that computer. If this policy setting is disabled or not configured, users of the same computer are allowed to establish their own security zone settings. The recommended state for this setting is: `Enabled`.

Rationale:

Users who change their Internet Explorer security settings could enable the execution of dangerous types of code from the Internet and Web sites that were listed in the Restricted Sites zone in the browser.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\Security_HKLM_only
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Zones: Use only machine settings
```

Impact:

Users will not be able to configure security settings for Internet Explorer zones.

Default Value:

Disabled

9 Additional Settings

9.1 Set 'Disable the Security page' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting works in conjunction with other settings to ensure that users cannot change the settings that are configured through Group Policy. This policy setting removes the Security tab from the Internet Options dialog box. If you enable this policy setting, users cannot view and change settings for security zones, such as scripting, downloads, and user authentication. The recommended state for this setting is: `Enabled`.

Rationale:

Users could change some of the Internet Explorer security settings, which could enable them to visit a malicious Web site and download or execute hostile code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control
Panel\SecurityTab
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Disable the Security page
```

Impact:

Users will be unable to view the Security Page.

Default Value:

Disabled

9.2 Set 'Disable the Advanced page' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting works in conjunction with other settings to ensure that users cannot change the settings that are configured in the Advanced tab of Internet Explorer. The recommended state for this setting is: `Enabled`.

Rationale:

Users could change some of the Internet Explorer security settings, which could enable them to visit a malicious Web site and download or execute hostile code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control
Panel\AdvancedTab
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Disable the Advanced page
```

Impact:

Users will no longer be able to access the Advanced page.

Default Value:

Disabled

9.3 Set 'Prevent downloading of enclosures' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer.

If you enable this policy setting, the user cannot set the Feed Sync Engine to download an enclosure through the Feed property page. A developer cannot change the download setting through the Feed APIs.

If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an enclosure through the Feed property page. A developer can change the download setting through the Feed APIs. The recommended state for this setting is: `Enabled`.

Rationale:

Enclosures could contain malicious payloads.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Feeds\DisableEnclosureDownload
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures
```

9.4 Set 'Turn on Basic feed authentication over HTTP' to 'Not Configured' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows users to have their feeds authenticated using the Basic authentication scheme over an unencrypted HTTP connection.

If you enable this policy setting, the RSS Platform will authenticate to servers using the Basic authentication scheme in combination with an insecure HTTP connection.

If you disable or do not configure this setting, the RSS Platform will not authenticate to servers using the Basic authentication scheme in combination with an insecure HTTP connection.

A developer cannot change this setting through the Feed APIs. The recommended state for this setting is: `Not Configured`.

Rationale:

Allowing basic authentication over HTTP for RSS feeds means that user credentials will be transmitted in plain text, they could be intercepted en route by a malicious user and either altered or copied.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Feeds\AllowBasicAuthInClear
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\RSS Feeds\Turn on
Basic feed authentication over HTTP
```

9.5 Configure 'Make proxy settings per-machine (rather than per-user)' (Not Scored)

Profile Applicability:

- Level 1

Description:

Applies proxy settings to all users of the same computer.

If you enable this policy, users cannot set user-specific proxy settings. They must use the zones created for all users of the computer.

If you disable this policy or do not configure it, users of the same computer can establish their own proxy settings.

This policy is intended to ensure that proxy settings apply uniformly to the same computer and do not vary from user to user.

This setting does not work when 32-bit versions of Internet Explorer are running on 64-bit versions of Windows. See the Microsoft Knowledgebase article "You cannot access the Internet through a proxy server when you use a 32-bit version of Internet Explorer on a computer that is running a 64-bit version of Windows" for more information on the issue and a method to work around it: http://support.microsoft.com/kb/952031. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

Enabling this policy setting ensures that proxy settings are applied uniformly to all users of the same computer.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet
Settings\ProxySettingsPerUser
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Make proxy settings per-machine (rather than per-user)
```

9.6 Configure 'Do not display the reveal password button' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to hide the reveal password button when Internet Explorer prompts users for a password. The reveal password button is displayed during password entry. When the user clicks the button, the current password value is visible until the mouse button is released (or until the tap ends).

If you enable this policy setting, the reveal password button will be hidden for all password fields. Users and developers will not be able to depend on the reveal password button being displayed in any web form or web application.

If you disable or do not configure this policy setting, the reveal password button can be shown by the application as a user types in a password. The reveal password button is visible by default.

On Windows 8 and later, if the "Do not display the reveal password button" policy setting located in Computer Configuration\Administrative Templates\Windows Components\Credential User Interface is enabled for the system, it will override this policy setting. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Main\DisablePasswordReveal
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Security Features\Do not display the reveal password button
```

9.7 Set 'Prevent changing proxy settings' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting specifies if a user can change proxy settings.

If you enable this policy setting, the user will not be able to configure proxy settings.

If you disable or do not configure this policy setting, the user can configure proxy settings. The recommended state for this setting is: `Enabled`.

Rationale:

Enabling this policy setting will prevent users from changing their proxy settings and potentially bypassing restrictions placed on Internet Explorer security zones, see http://msdn.microsoft.com/en-us/library/bb250483(v=VS.85).aspx for more information.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control Panel\Proxy
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Prevent changing proxy settings
```

9.8 Configure 'Disable changing Automatic Configuration settings' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting removes a user's ability to change automatically configured settings. Administrators use automatic configuration to update browser settings periodically. If you

enable this policy setting, the automatic configuration settings are dimmed in Internet Explorer. (These settings are located in the Automatic Configuration area of the LAN Settings dialog box.) This policy setting also removes a user's ability to change settings that are configured through Group Policy. To view the LAN Settings dialog box

1. Open the Internet Options dialog box, and click the Connections tab.
2. Click the LAN Settings button to view the settings.

Note: The Disable the Connections page setting removes the Connections tab from Internet Explorer in Control Panel and takes precedence over this Disable changing Automatic Configuration settings configuration option. If the former setting is enabled, the latter setting is ignored. The Disable the Connections page setting is located in `\User Configuration \Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel` in the Group Policy Object Editor. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

Users could change some of the Internet Explorer security settings, which could enable users to visit a malicious Web site and download or execute hostile code.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Control Panel\Autoconfig
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Disable changing Automatic Configuration settings
```

Impact:

Users will be unable to change the automatic configuration settings.

Default Value:

Disabled

9.9 Set 'Prevent "Fix settings" functionality' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting prevents users from performing the "Fix settings" functionality related to the Security Settings Check in Internet Explorer. The recommended state for this setting is: `Disabled`.

Rationale:

The "Fix settings" feature is an easy way for users to restore secure settings for Internet Explorer should the settings be misconfigured in some way, disabling will prevent users from quickly returning the browser to its default configuration.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Security\DisableFixSecuritySettings
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Prevent "Fix settings" functionality
```

Impact:

If you enable this policy setting, users cannot click the Fix Settings For Me option in the Information bar context menu that appears when Internet Explorer determines that its configuration is not secure.

Default Value:

Disabled

9.10 Set 'Turn off the Security Settings Check feature' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting turns off the Security Settings Check feature, which checks Internet Explorer security settings to determine when the settings put Internet Explorer at risk. The recommended state for this setting is: `Disabled`.

Rationale:

If the Security Settings Check feature is disabled then users will not be warned if their security settings are configured in such a way that Internet Explorer is at risk of compromise.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Security\DisableSecuritySettingsCheck
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Turn off the Security Settings Check feature
```

Impact:

If you enable this policy setting, the security settings check will not be performed. If you disable this policy setting, the security settings check will be performed. If you do not configure this policy setting, the user will be able to change the "Disable Security Settings Check" setting.

Default Value:

Disabled

9.11 Configure 'Disable changing connection settings' (Not Scored)

Profile Applicability:

- Level 1

Description:

This policy setting removes users' ability to change dial-up settings. If you enable this policy setting, the Settings button on the Connections tab in the Internet Options dialog box is dimmed. This policy setting also removes users' ability to change settings that are configured through Group Policy. You may want to disable this policy setting for laptop users if their travel requires them to change their connection settings. Configure this setting in a manner that is consistent with security and operational requirements of your organization.

Rationale:

Users could alter existing connections to make it impossible for them to use Internet Explorer to browse some, or all, Web sites.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Not Configured`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Disable changing connection settings
```

Impact:

Users will be unable to change the connection settings.

Default Value:

Disabled

9.12 Set 'Turn off Crash Detection' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to manage the crash detection feature of add-on management in Internet Explorer. If you enable this policy setting, a crash in Internet Explorer will be similar to one on a computer that runs Windows XP Professional with Service Pack 1 (SP1) or earlier: Windows Error Reporting will be invoked. If you disable this policy setting, the crash detection feature in add-on management will be functional. If you experience frequent repeated crashes and need to report them for follow-up troubleshooting, you could temporarily configure the policy setting to Disabled. The recommended state for this setting is: `Enabled`.

Rationale:

A crash report might contain sensitive information from the computer's memory.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Restrictions\NoCrashDetection
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Turn off Crash Detection
```

Impact:

Information about crashes that are caused by Internet Explorer add-ons will not be reported to Microsoft. If you experience frequent repeated crashes and need to report them to help troubleshoot the problem, the setting should temporarily be changed to Disabled.

Default Value:

Disabled

9.13 Set 'Disable AutoComplete for forms' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls automatic completion of fields in forms on Web pages. If you enable this policy setting, the AutoComplete feature will not suggest possible choices for completing a form. This can help protect sensitive data in certain environments. The recommended state for this setting is: `Enabled`.

Rationale:

It is possible that this feature will cache sensitive data and store it in the user's profile where it might not be protected as rigorously as required by organizational policy.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\Software\Policies\Microsoft\Internet Explorer\Main\Use FormSuggest
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Enabled`.

```
User Configuration\Administrative Templates\Windows Components\Internet
Explorer\Disable AutoComplete for forms
```

Impact:

If you enable this policy setting, the AutoComplete feature will not suggest possible choices for completing a form.

Default Value:

Disabled

9.14 Set 'Turn on the auto-complete feature for user names and passwords on forms' to 'Disabled' (Scored)

Profile Applicability:

- Level 1

Description:

This AutoComplete feature can remember and suggest User names and passwords on Forms.

If you enable this setting, the user cannot change "User name and passwords on forms" or "prompt me to save passwords". The Auto Complete feature for User names and passwords on Forms will be turned on. You have to decide whether to select "prompt me to save passwords".

If you disable this setting the user cannot change "User name and passwords on forms" or "prompt me to save passwords". The Auto Complete feature for User names and passwords on Forms is turned off. The user also cannot opt to be prompted to save passwords.

If you do not configure this setting, the user has the freedom of turning on Auto complete for User name and passwords on forms and the option of prompting to save passwords. To display this option, the users open the Internet Options dialog box, click the Contents Tab and click the Settings button. The recommended state for this setting is: `Disabled`.

Rationale:

It is possible that malware could be developed which would be able to extract the cached user names and passwords from the currently logged on user, which an attacker could then use to compromise that user's online accounts.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\Software\Policies\Microsoft\Internet Explorer\Main\FormSuggest
Passwords
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to `Disabled`.

```
User Configuration\Administrative Templates\Windows Components\Internet Explorer\Turn
on the auto-complete feature for user names and passwords on forms
```

Impact:

If you disable this policy setting, the check boxes for User Names and Passwords on Forms and Prompt Me to Save Passwords are dimmed and users are prevented from saving passwords locally.

Default Value:

Disabled

9.15 Set 'Turn on 64-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows' to 'Enabled' (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether Internet Explorer 11 uses 64-bit processes (for greater security) or 32-bit processes (for greater compatibility) when running in Enhanced Protected Mode on 64-bit versions of Windows.

If you enable this policy setting, Internet Explorer 11 will use 64-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows.

If you disable this policy setting, Internet Explorer 11 will use 32-bit tab processes when running in Enhanced Protected Mode on 64-bit versions of Windows.

If you don't configure this policy setting, users can turn this feature on or off using Internet Explorer settings. This feature is turned off by default.

Rationale:

Enabling 64-bit tab processes will improve the efficacy of exploit mitigations, such as Address Space Layout Randomization (ASLR).

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main\Isolation64Bit
```

Remediation:

To establish the recommended configuration via Group Policy, set the following UI path to Enabled.

```
Computer Configuration\Administrative Templates\Windows Components\Internet
Explorer\Internet Control Panel\Advanced Page
```

Impact:

Some ActiveX controls and toolbars may not be available when 64-bit processes are used.

Appendix: Change History

Date	Version	Changes for this version
12-01-2014	1.0.0	Initial Release