Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	**CSO-STD-1422**
Office Instruction Title:	**Microsoft Internet Explorer 9 Configuration Standard**
Revision Number:	**1.0**
Effective Date:	June 1, 2014
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PST**
Summary of Changes:	CSO-STD-1422, "Microsoft Internet Explorer 9 Configuration Standard" provides the minimum configuration settings that must be applied to NRC computing assets running Microsoft Internet Explorer 9.
Training:	As requested
ADAMS Accession No.:	ML14016A254

Approvals				
Primary Office Owner	Policies, Standards, and Training		**Signature**	**Date**
Standards Working Group Chair	Bill Dabbs		**/RA/**	**2/20/2014**
Responsible SITSO	Kathy Lyons-Burke		**/RA/**	**2/20/2014**
DAA for Non-major IT Investments	Director, CSO	Tom Rich	**/RA/**	**2/24/2014**
	Director, OIS	Jim Flanagan	**/RA/**	**3/5/2014**

TABLE OF CONTENTS

List of Tables

Computer Security Standard
CSO-STD-1422

Microsoft Internet Explorer 9 Configuration Standard

1 PURPOSE

CSO-STD-1422, "Microsoft®[1] Internet Explorer 9 Configuration Standard" provides required configuration settings for the Nuclear Regulatory Commission (NRC) computing assets running Microsoft Internet Explorer (IE) 9. These settings serve to minimize the probability of NRC sensitive information compromise. The standard applies to computing assets used to process Sensitive Unclassified Non-Safeguards Information (SUNSI) and Safeguards Information (SGI).

This configuration standard is intended for system administrators and information system security officers (ISSOs) that have the required knowledge, skills, and abilities to apply configuration settings to IE 9.

2 GENERAL REQUIREMENTS

All NRC computing assets (e.g., servers, workstations, laptops) running IE 9 that are owned, managed, and/or operated by the NRC or by other parties on behalf of the NRC must comply with this standard as a minimum set of controls. Additional controls may be required after a system risk analysis is completed.

The IE 9 configurations on computing assets operated by the NRC or other parties on behalf of the NRC must comply with the Defense Information Systems Agency (DISA) Microsoft IE 9 Security Technical Implementation Guide (STIG), as modified by the requirements provided in this standard. The effective version of the DISA STIG is specified on the Computer Security Office (CSO) Standards Web page.

2.1 Patch Application

All available patches and security updates must be applied to IE 9 before being placed into an NRC computing environment (e.g., development, test, production).

Patches must be applied on an ongoing basis per the requirements specified in CSO-STD-0020, "Organization Defined Values for System Security Controls." This ensures that known vulnerabilities are remediated on a regular schedule.

[1] Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

3 SPECIFIC REQUIREMENTS

This section provides requirements that differ from or are required in addition to those published in the DISA Microsoft IE 9 STIG.

3.1 NRC Modifications to the DISA STIG

The following sections provide guidance in applying the DISA STIG to the NRC and the DISA STIG configuration setting modified to be NRC-specific.

Many of the IE STIG requirements involve Java settings. These Java settings are Microsoft Java settings, not Oracle Java. Please note that Microsoft Java has been deprecated since July 1, 2009.

3.1.1 DISA STIG Term Equivalence

To understand how to comply with the DISA Microsoft IE 9 STIG, system administrators must substitute the NRC terms supplied in Table 3.1-1, DISA Microsoft IE 9 STIG and NRC Terms, for the equivalent terms used throughout the STIG.

Table 3.1-1: DISA Microsoft IE 9 STIG and NRC Terms

DISA STIG Terms	NRC Terms
DoD (Department of Defense)	NRC
Information Assurance Manager (IAM), Information Assurance Officer (IAO), Network Security Officer (NSO), and Site Representative	ISSO
Mission Assurance Category (MAC-1)	Systems with a Federal Information Processing Standard (FIPS)-199 High Sensitivity Level
Mission Assurance Category (MAC-2)	Systems with a FIPS-199 Moderate Sensitivity Level
Mission Assurance Category (MAC-3)	Systems with a FIPS-199 Low Sensitivity Level

3.1.2 Requirement that is Different from the DISA STIG

This section provides the NRC-specific requirement that is different from the published DISA STIG requirements. In Table 3.1-2, IE 9 NRC-Specific Requirement that is Different from the DISA STIG, the section header matches the header in the DISA STIG.

The following defines the information contained within the columns of Table 3.1-2:

- Step: The unique identifier of this configuration item within this standard.
- STIG ID: The DISA STIG identifier (ID) number for this configuration item.
- Setting Name: The configuration item or issue.
- DISA Setting: The configuration setting per the DISA STIG.
- NRC-Specific Requirement: The NRC setting (which is different from the DISA STIG requirement) for a configuration item.

- Rationale: The rationale for the NRC-specific requirement that is different from the published setting in the DISA STIG.

Table 3.1-2: IE 9 NRC-Specific Requirement that is Different from the DISA STIG

Step	STIG ID	Setting Name	DISA Setting	NRC-Specific Requirement	Rationale
Encryption					
1.	DTBI014	DTBI014- IE SSL/TLS Settings	Secure Socket Layer (SSL) 3.0 and Transport Layer Security (TLS) 1.0 must be selected. SSL 2.0 must not be used.	Configure client encryption per the requirements in CSO-STD-2009.	NRC encryption requirements are specified in CSO-STD-2009, "Cryptographic Control Standard."

3.2 Security Zones

System administrators must not disable the IE 9 security zones. IE 9 includes predefined security zones with preset default levels of security to manage a secure environment.

- **Internet Zone** - By default, all Internet and intranet sites are assigned to the Internet zone. Intranet sites are not part of the Local Intranet zone unless the user explicitly adds them to this zone.
- **Local Intranet Zone** - The Local Intranet zone contains all network connections that are established using a Universal Naming Convention (UNC) path, Web sites that bypass proxy servers or have names that do not include periods (for example, http://local), as long as they are not assigned to the Restricted Sites or Trusted Sites zones.
- **Trusted Sites Zone** - The Trusted Sites zone contains Web sites that are deemed safe (e.g., Web sites that are on the intranet or from established trusted companies).
- **Restricted Sites Zone** - The Restricted Sites zone contains Web sites that are not trusted.

3.2.1 Trusted Sites Zone

System administrators must change the level of security for each IE 9 security zone in compliance with the DISA Microsoft IE 9 STIG. Security zones offer a method to enforce Internet security policies, based on the origin of the Web content.

The Internet zone is the default zone for all Web sites unless otherwise configured. The system administrator must lock down the Internet zone as a first line of defense against potentially dangerous Web sites. A tightly configured Internet zone will cause some Web sites to not operate normaly by default. By adding the Web site to the Trusted Sites zone, a set of privacy and security policies less restrictive than the Internet zone is used.

The level of security set for the Trusted Sites zone is applied to sites that are specifically indicated to be trusted not to damage the computing asset or information. The Trusted Sites security zone is reserved for sites that are trusted and require additional capabilities that are not configured in the Internet, Local Intranet, or Restricted Sites security zones. For example:

- ActiveX is a form of mobile code. ActiveX can be used to embed multimedia content into other applications such as Microsoft Office or IE. ActiveX plug-ins (e.g., Adobe Flash) will not display properly unless the Web site displaying the content is added to the Trusted Sites zone.
- Web sites in the Trusted Sites zone are permitted to download Web content and files.

If there is a business need, the system and network ISSO can authorize specific sites in the Trusted Sites zone. The authorization and rationale supporting the need to add a site in the Trusted Sites zone must be documented.

3.3 Additional Windows Server Requirements

This section defines specific requirements for Windows servers only.

3.3.1 Internet Browsing on Windows Servers

Browsing the Internet on servers can expose the server to malicious code obtained from Web site content. Due to the criticality of servers providing services for business operations (e.g., Domain services, print server, file server), the network must ensure that Internet browsing capabilities on all Windows server types are prohibited with the following exemption:

- The following Windows server type is exempt from being blocked:
  - Windows Server Update Services (WSUS) Server

If there is a business need, the system and network ISSO can authorize specific servers to access the Internet via the Web browser. The authorization and rationale supporting the need for Web browsing on the server must be documented.

Intranet browsing (e.g., SharePoint, Internet Web applications) is permitted on Windows servers.

4 DEFINITIONS

ActiveX	A software framework created by Microsoft that adapts its earlier Component Object Model (COM) and Object Linking and Embedding (OLE) technologies for content downloaded from a network, particularly in the context of the World Wide Web.
Computing Asset	Any hardware device or component of the environment that supports information-related activities.
Enhanced Security Configuration	A Windows add-on feature for Windows Server 2003 and later that enables a locked down version of IE 9.
Trusted Sites	IE 9 security zone for the Internet sites whose content the user trusts.
Restricted Sites	IE 9 security zone contains sites the user does not trust.

5 ACRONYMS

CAT	Severity Category Code
COM	Component Object Model
CSO	Computer Security Office
DISA	Defense Information Systems Agency
DoD	Department of Defense
ESC	Enhanced Security Configuration
FIPS	Federal Information Processing Standard
IAM	Information Assurance Manager
IAO	Information Assurance Officer
ID	Identifier
IE	Internet Explorer
MAC	Mission Assurance Category
ISSO	Information System Security Officer
NRC	Nuclear Regulatory Commission
NSO	Network Security Officer
OIS	Office of Information Services
OLE	Object Linking and Embedding
PST	Policies Standards and Training
SGI	Safeguards Information
SITSO	Senior Information Technology Security Officer
SSL	Secure Socket Layer
STD	Standard
STIG	Security Technical implementation Guide
SUNSI	Sensitive Unclassified Non-Safeguards Information
TLS	Transport Layer Security

UNC	Universal Naming Convention
WSUS	Windows Server Update Services

APPENDIX A. METHOD FOR IMPLEMENTING MICROSOFT IE 9

A.1 Enhanced Security Configuration (ESC)

The ESC automated mechanism tool can help system administrators to implement the required IE 9 security configurations specified in this standard and secure IE 9. ESC is a Windows add-on feature for Windows Server 2003 and later that enables a locked down configuration of IE 9. ESC increases the security of IE 9 and reduces the risk of attack from Web-based insecure content.

ESC is enabled by default for Windows Servers. Enabling ESC configures IE 9 with higher security settings for the built-in security zones than a non-ESC enabled IE 9. ESC will allow for additional security configurations to be made to support security, however ESC will not permit a setting preconfigured by ESC to be configured to a less secure value.

System administrators must:

- Implement ESC for IE 9 on servers and enable for both system administrators and users.
- Configure ESC through the Add/Remove Windows Components area for Windows Server 2003 and in the Server Manager console under “Configure IE ESC” for Windows Server 2008.
- Enable ESC to assist in hardening a portion of the IE 9 requirements. For example, by enabling ESC for both users and system administrators, 64 of the 133 checks (48%) in the DISA Microsoft IE 9 STIG are configured automatically.[2]

Table A.1-1, DISA STIG Requirements Addressed by Enabling ESC, lists the DISA STIG IDs that will be addressed when ESC is enabled. The following defines the information contained within the columns of Table A.1-1:

- STIG ID: The DISA STIG ID number for this configuration item.
- Severity: The DISA Severity Category Code (CAT) level assigned for this configuration item. CAT-I findings are of the highest severity, while CAT-III findings are the lowest.
- Rule Title: The title of the configuration item.

Table A.1-1: DISA STIG Requirements Addressed by Enabling ESC

STIG ID	Severity	Rule Title
DTBI022	CAT II	The Download signed ActiveX controls property must be disallowed (Internet zone).
DTBI023	CAT II	The Download unsigned ActiveX controls property must be disallowed (Internet zone).
DTBI024	CAT II	The Initialize and script ActiveX controls not marked as safe property must be disallowed (Internet zone).
DTBI030	CAT II	Font downloads must be disallowed (Internet zone).
DTBI032	CAT II	Accessing data sources across domains must be disallowed (Internet zone).

[2] Per the version of the DISA STIG used in the creation of this standard, DISA Microsoft Internet Explorer 9 STIG V1R6.

STIG ID	Severity	Rule Title
DTBI036	CAT II	Functionality to drag and drop or copy and paste files must be disallowed (Internet zone).
DTBI038	CAT II	Launching programs and files in IFRAME must be disallowed (Internet zone).
DTBI039	CAT II	Navigating windows and frames across different domains must be disallowed (Internet zone).
DTBI042	CAT II	Userdata persistence must be disallowed (Internet zone).
DTBI044	CAT II	Clipboard operations via script must be disallowed (Internet zone).
DTBI046	CAT II	Logon options must be configured to prompt (Internet zone).
DTBI112	CAT II	The Download signed ActiveX controls property must be disallowed (Restricted Sites zone).
DTBI113	CAT II	The Download unsigned ActiveX controls property must be disallowed (Restricted Sites zone).
DTBI114	CAT II	The Initialize and script ActiveX controls not marked as safe property must be disallowed (Restricted Sites zone).
DTBI115	CAT II	ActiveX controls and plug-ins must be disallowed (Restricted Sites zone).
DTBI116	CAT II	ActiveX controls marked safe for scripting must be disallowed (Restricted Sites zone).
DTBI119	CAT II	File downloads must be disallowed (Restricted Sites zone).
DTBI120	CAT II	Font downloads must be disallowed (Restricted Sites zone).
DTBI122	CAT II	Accessing data sources across domains must be disallowed (Restricted Sites zone).
DTBI123	CAT II	The Allow META REFRESH property must be disallowed (Restricted Sites zone).
DTBI127	CAT II	Installation of desktop items must be disallowed (Restricted Sites zone).
DTBI128	CAT II	Launching programs and files in IFRAME must be disallowed (Restricted Sites zone).
DTBI129	CAT II	Navigating windows and frames across different domains must be disallowed (Restricted Sites zone).
DTBI132	CAT II	Userdata persistence must be disallowed (Restricted Sites zone).
DTBI133	CAT II	Active scripting must be disallowed (Restricted Sites zone).
DTBI134	CAT II	Clipboard operations via script must be disallowed (Restricted Sites zone).
DTBI136	CAT II	Logon options must be configured and enforced (Restricted Sites zone).
DTBI340	CAT II	Active content from CDs must be disallowed to run on user machines.
DTBI350	CAT II	Software must be disallowed to run or install with invalid signatures.
DTBI355	CAT II	Third-party browser extensions must be disallowed.
DTBI365	CAT II	Checking for server certificate revocation must be enforced.
DTBI370	CAT II	Checking for signatures on downloaded programs must be enforced.
DTBI385	CAT II	Script-initiated windows without size or position constraints must be disallowed (Internet zone).
DTBI390	CAT II	Script-initiated windows without size or position constraints must be disallowed (Restricted Sites zone).
DTBI395	CAT II	Scriptlets must be disallowed (Internet zone).

STIG ID	Severity	Rule Title
DTBI415	CAT II	Automatic prompting for file downloads must be disallowed (Internet zone).
DTBI455	CAT II	Loose XAML files must be disallowed (Internet zone).
DTBI460	CAT II	Loose XAML files must be disallowed (Restricted Sites zone).
DTBI465	CAT II	MIME sniffing must be disallowed (Internet zone).
DTBI470	CAT II	MIME sniffing must be disallowed (Restricted Sites zone).
DTBI495	CAT II	Pop-up Blocker must be enforced (Internet zone).
DTBI500	CAT II	Pop-up Blocker must be enforced (Restricted Sites zone).
DTBI515	CAT II	Web sites in less privileged Web content zones must be disallowed to navigate into the Internet zone.
DTBI520	CAT II	Web sites in less privileged Web content zones must be disallowed to navigate into the Restricted Sites zone.
DTBI575	CAT II	Allow binary and script behaviors must be disallowed (Restricted Sites zone).
DTBI580	CAT II	Automatic prompting for file downloads must be disallowed (Restricted Sites zone).
DTBI650	CAT II	.NET Framework-reliant components not signed with Authenticode must be disallowed to run (Restricted Sites zone).
DTBI655	CAT II	.NET Framework-reliant components signed with Authenticode must be disallowed to run (Restricted Sites zone).
DTBI670	CAT II	Scripting of Java applets must be disallowed (Restricted Sites zone).
DTBI800	CAT II	Scripting of IE Web browser control property must be disallowed (Internet zone).
DTBI810	CAT II	When uploading files to a server, the local directory path must be excluded (Internet zone).
DTBI820	CAT II	Launching programs and unsafe files property must be set to prompt (Internet zone).
DTBI830	CAT II	ActiveX controls without prompt property must be used in approved domains only (Internet zone).
DTBI840	CAT II	Cross-Site Scripting (XSS) Filter must be enforced (Internet zone).
DTBI850	CAT II	Scripting of IE Web Browser Control must be disallowed (Restricted Sites zone).
DTBI860	CAT II	When uploading files to a server, the local directory path must be excluded (Restricted Sites zone).
DTBI870	CAT II	Launching programs and unsafe files property must be set to prompt (Restricted Sites zone).
DTBI880	CAT II	ActiveX controls without prompt property must be used in approved domains only (Restricted Sites zone).
DTBI890	CAT II	Cross-Site Scripting (XSS) Filter property must be enforced (Restricted Sites zone).
DTBI910	CAT II	Status bar updates via script must be disallowed (Internet zone).
DTBI920	CAT II	.NET Framework-reliant components not signed with Authenticode must be disallowed to run (Internet zone).
DTBI930	CAT II	.NET Framework-reliant components signed with Authenticode must be disallowed to run (Internet zone).
DTBI940	CAT II	Scriptlets must be disallowed (Restricted Sites zone).

STIG ID	Severity	Rule Title
DTBI950	CAT II	Status bar updates via script must be disallowed (Restricted Sites zone).

CSO-STD-1422 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
16-Jan-14	1.0	Initial Release	CSO Web page and notification forum	Upon request