Date Originated: 5 MAR 2009 Drafted By: IT1(SW) Kangas Date Reviewed: Reviewed By:

Title: USS JOHN PAUL JONES (DDG 53) CC DIVISION

Suffix: INFORMATION SYSTEMS STANDARD OPERATING PROCEDURES ISNS-013

Subject: CONFIGURING WEB BROWSER TO ALLOW NSIPS AFLOAT DOWNLOADS.

<u>Purpose</u>: To promulgate procedures for configuring the NSIPS Afloat web portal to allow download of embedded Microsoft Excel spreadsheets in the CIMS application.

Background: This procedure is a workaround and modification to the browser settings and group policy objects in the Compose 3.0 environment. This action should be taken when users encounter error messages attempting to open generated Excel spreadsheets.

<u>Action</u>:

1. On DC01, open the group policy editor by clicking start \rightarrow run and typing in "gpmc.msc" to open the group policy editor NOTE: You must be logged in with administrative credentials:

Run	? 🗙
1	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	gpmc.msc
	OK Cancel <u>B</u> rowse

2. Drill down the left hand pane to Group Policy Objects. Expand the list of group policy objects, and highlight Compose Domain Policy. Right click and select edit to bring up the group policy editor.

Sroup Policy Management		_ & ×			
ිදී Eile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp		_ 8 ×			
양을 Group Policy Management 금~슈 Forest: ddg53.navy.mil	COMPOSE Domain Policy				
Domains	Scope Details Settings Delegation	1			
COMPOSE Domain Policy	Network/SNMP	<u>show</u>			
COMPOSE Domain-Unclass Policy	Printers	<u>show</u>			
COMPOSE User Settings Policy	System	<u>show</u>			
Derault Domain Policy GOMPOSE Users and Computers	System/Error Reporting	show			
🗈 🔯 Domain Controllers	System/Group Policy	show			
Group Policy Objects	System/Internet Communication Management/Internet Communication settings	show			
COMPOSE Domain Controllers Polic	System/Logon	show			
COMPOSE Domain Policy	System/Remote Assistance	show			
COMPOSE Domain-Unclass Policy	System/User Profiles	show			
COMPOSE User Settings Policy	Windows Components/Internet Explorer	show			
COMPOSE Workstations Policy	Windows Components/Internet Explorer/Internet Control Panel/Security Page/Internet Zone	show			
	Windows Components/Internet Explorer/Internet Control Panel/Security Page/Intranet Zone	show			
Disable USB Storage Devices	Windows Components/Internet Explorer/Internet Control Panel/Security Page/Restricted Sites Zone	show			
Enable USB Storage Devices (Exce	Windows Components/Internet Explorer/Internet Control Panel/Security Page/Trusted Sites Zone	show			
	Windows Components/NetMeeting	show			
III Scotts Background	Windows Components/Task Scheduler	show			
😟 🕞 WMI Filters	Windows Components/Terminal Services	show			
Group Policy Modeling	Windows Components/Terminal Services/Encryption and Security	show			
Group Policy Results	Windows Components/Terminal Services/Sessions	show			
	Windows Components/Terminal Services/Temporary folders	show			
	Windows Components/Windows Installer	show			
	Windows Components/Windows Media Player	show			
	Windows Components/Windows Messenger	show			
	Extra Registry Settings	show			
	User Configuration (Enabled)	hide			
	Windows Settings	hide			
	Security Settings	show			
	Folder Redirection	show			
	Internet Explorer Maintenance	show			
T					

3. Drill down to the security page property under computer configuration \rightarrow Administrative Templates \rightarrow Internet Control Panel:

🚡 Group Policy Object Editor			
Eile Action View Help			
COMPOSE Domain Policy [ddg53uopdc01.ddg53.navy.ml] Computer Configuration Computer Settings Computer Settings Components	Security Page Site to Zone Assignment List Display Properties Requirements: at least Internet Explorer v6.0 in Windows XP Service Pack 2 or Windows Server 2003 Service Pack 1 Description: This policy setting alows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone. Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zones (1) Intranet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone Kite to these zone (Medium-Low template), And Restricted Sites zone Kite to these zone (Medium template), And Restricted Sites zone Kite to these zone (Medium template), And Restricted Sites zone Kite to these zone Kite to these zone (Medium template), Site to the security Extended & Standard	Setting Internet Zone Cocked-Down Internet Zone Cocked-Down Intranet Zone Cocked-Down Trusted Sites Zone Cocked-Down Trusted Sites Zone Cocked-Down Internet Zone Cocked-Down Local Machine Zone Template Cocked-Down Internet Zone Templat	Enable: Enable: Not config. Not config.

4. Double click on Site to zone assignment list (This adds sites to each the security settings) Make sure the setting tab is set to enabled.

Site to Zone Assignment List Properties	X
Setting Explain	
🗿 Site to Zone Assignment List	
 Not Configured Enabled Disabled 	
Enter the zone assignments here. Show	
Supported on: at least Internet Explorer v6.0 in Windows XP Service Previous Setting Next Setting	
OK Cancel Apply	

5. Click on the **show**... button to display the zone mappings. You will see a list of sites that are in approved zones for security settings.

Show Contents Enter the zone assignments here.		ОК
Value Name http://ddg53usv01 http://nsipswebafloat http://nsipswebafloat.ddg53.navy.mil https://seat1.nmci.navy.mil	Value 1 2 2 2	Cancel
https://seat2.nmci.navy.mil radpac.cdmd.navy.mil seat1.cpf.navy.mil seat2.cpf.navy.mil www.cdmd.navy.mil	2 2 2 2 2	Add

6. Click on the Add button. Add the url and zone mapping as follows:

Add Item	×
Enter the <u>n</u> ame of the item to be added:	OK
nsipswebafloat	Cancel
Enter the value of the item to be added:	
2	

7. Click OK. Click on Add again to add the FQDN for your NSIPS Afloat server:

Add Item	×
Enter the <u>n</u> ame of the item to be added:	OK
nsipswebafloat.ddg53.navy.mi	Cancel
Enter the value of the item to be added:	
2	

8. Replace ddg53.navy.mil with the hullnumber.navy.mil address for your site.

9. Click on OK on the Show Contents Dialog box. Click OK on the site to zone assignment properties box.

10. Drill down under user configuration→Administrative Templates→Windows Components→Internet Explorer→Internet Control Panel→Security Page.

11. Enter the sites in the site to zone assignment list property as in steps 4 through 9 above.

12. Next, select the Internet Explorer folder, and double click the disable changing advanced page settings property. Ensure that the property is configured as "Not Configured"

🚡 Group Policy Object Editor				
<u>File Action View H</u> elp				
User Configuration Software Settings Software Settings Windows Settings Soripts (Logon/Logoff) Socurity Settings Folder Redirection Software Explorer Maintenance Software Explorer Maintenance Software Settings Software Settings Software Explorer Maintenance Software Settings Software Settings Software Explorer Maintenance Software S		Internet Explorer Disable changing Advanced page settings Display Properties Requirements: at least Internet Explorer v5.0 Description: Prevents users from changing settings on the Advanced tab in the Internet Options dialog box. If you enable this policy, users are prevented from changing advanced Internet settings, such as security, multimedia, and printing. Users cannot select or clear the check boxes on the Advanced tab. If you disable this policy or do not configure it, users can select or clear settings on the Advanced tab. If you disable this policy or do not configure it, users can select or clear settings on the Advanced tab. If you set the "Disable the Advanced Explorer/Internet Control Panel), you do not need to set this policy. The provide the set of this policy, Display Property (Internet Control Panel), you do not need to set this policy. The prevents of the policy. Display Property Provide this policy. Display Provide th	Setting Internet Control Panel Offline Pages Browser menus Toolbars Persistence Behavior Administrator Approved Controls Security Features Search: Disable Find Files via F3 within the browser Disable external branding of Internet Explorer Disable external branding of Internet Explorer Disable changing home page settings Disable changing forme page settings Disable changing forme page settings Disable changing formerary Internet Files settings Disable changing networks works settings Disable changing networks works settings Disable changing file color settings Disable changing networks vertings Disable changing not settings Disable changing language settings	State A Not configu Not configu
	-			

14. Close out of the group policy editor.

15. From a command prompt, type "gpupdate /force" to push the updated policy across the network. The rest of the configuration is made on the users machine.

16. Now, you will need to go to the users computer that is experiencing downloading problems within NSIPS Afloat. NOTE: The following changes must be made under the user account name that is having difficulty. The changes are specific to the users profile.

17. From the user workstation, open internet explorer. Click on the tools menu, and select internet options:



18. Click on the security tab, and highlight the trusted sites zone:

Internet Option	s	<u>? ×</u>
General Secu	rity Privacy Content Conn	ections Programs Advanced
Select a Web	content zone to specify its secu	urity settings.
	(1)	
Internet	Local intranet Trusted site	Restricted sites
Trusto This zo trust no data. Security leve Mo	ed sites one contains Web sites that you of to damage your computer or el for this zone ve the slider to set the security	l <u>S</u> ites
Lo	Minimal safeguards and warnin Most content is downloaded ar All active content can run Appropriate for sites that you al <u>Custom Level</u>	ng prompts are provided nd run without prompts bsolutely trust Default Level
	OK	Cancel Apply

19. Click on Sites… button to show the sites in your trusted sites zone. Ensure that your NSIPS server addresses are listed. If the sites are not listed, the user must log out and log back into the computer to refresh the group policies on the workstation.

Trusted sites	<u>?</u> ×
You can add and remove Web sites from this zon in this zone will use the zone's security settings.	ne. All Web sites
Add this Web site to the zone:	
	<u>A</u> dd
<u>W</u> eb sites:	
http://nsipswebafloat.ddg53.navy.mil radpac.cdmd.navy.mil seat1.cpf.navy.mil https://seat1.nmci.navy.mil seat2.cpf.navy.mil https://seat2.nmci.navy.mil	<u>R</u> emove
Require server verification (https:) for all sites in this	zone
ОК	Cancel

20. Ensure that the require server verification (https: for all sites in this zone checkbox is unchecked.

21. Close the trusted sites dialog box, and click on the advanced tab of the internet options dialog box:

Internet Options	×
General Security Privacy Content Connections Programs Advance	ed
Settings:	1
OK Cancel Apply	

22. Under browsing, ensure that the "Enable Folder View for FTP sites" checkbox is blank.

22. Ensure that the "Use Passive FTP (for firewall and DSL modem capability)" check box is checked.

Internet Options	×
General Security Privacy Content Connections Programs Advanced	1
Settings:	
 Always Hover Never Use inline AutoComplete Use Passive FTP (for firewall and DSL modem compatibility) Use smooth scrolling HTTP 1.1 settings Use HTTP 1.1 Use HTTP 1.1 through proxy connections Java (Sun) Use JRE 1.5.0_15 for <applet> (requires restart)</applet> Multimedia Enable Automatic Image Resizing Enable Image Toolbar (requires restart) Play animations in web pages Play sounds in web pages Restore Defaults 	
OK Cancel Apply	

23. Under security, ensure the "Allow active content from CDs to run on My Computer" and "Allow active content to run in files on My Computer" check boxes are checked.

Internet Options	×
General Security Privacy Content Connections Programs Advance	d
<u>S</u> ettings:	
 Do not search from the Address bar Just display the results in the main window Just go to the most likely site Security Allow active content from CDs to run on My Computer Allow active content to run in files on My Computer Allow software to run or install even if the signature is invalid Check for publisher's certificate revocation Check for signatures on downloaded programs Do not save encrypted pages to disk Empty Temporary Internet Files folder when browser is closed Enable Integrated Windows Authentication (requires restart) Enable Profile Assistant Use SSL 2.0 Use SSL 3.0 	
OK Cancel Apply	

24. Click on OK to close the dialog box. You should now be able to log into the NSIPS Web afloat portal, and download Microsoft Excel Spreadsheets from the CIMS application.