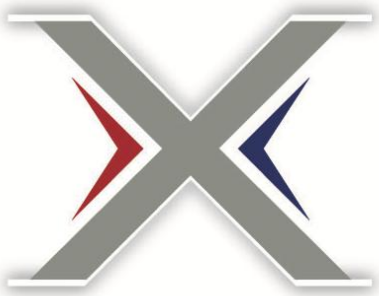

Gray Cell Rules of Engagement

Version 3.0

Purpose of this Document

This specification serves as a guide for Gray Cell activities in support of Cyber Defense Exercise 2016 (CDX 2016).

Document Revision History

Version	Change Description	Change Owner	Date
1.0	2015 FINAL VERSION	James Overby, LTJG, USN	20 Mar 2015
3.0	FINAL	Jim Titcomb	12 Feb 2016

1.0 Gray Cell Rules of Engagement

1.1 The following Rules of Engagement are binding on all members of the CDX 2016 Gray Cell. Members will be expected to sign a statement acknowledging that they have read and understood these Rules of Engagement.

2.0 CDX 2016 Gray Cell Policy

2.1 The Gray Cell will simulate normal network activity across the Blue Cell enclaves in order to assist White Cell in monitoring Blue Cell compliance with the Exercise Directive. All Gray Cell actions must be approved by Gray Cell Team Lead at CDX HQ prior to each attempt.

2.2 Members of the Gray Cell will work to simulate legitimate operations as a “user” and/or trusted third party operator. Gray Cell users will act as "trusted insiders" for each BLUENET: simulating user activity inside each Blue Cell user enclave. This function may be augmented by simulation software that is installed on Blue Cell hosts and monitored by Gray Cell members at HQ.

2.3 Gray Cell will remotely access the Gray Cell workstations within each BLUENET from CDX HQ via Remote Desktop Protocol (RDP) or Secure Shell Protocol (SSH) via a relay host. The relay host will be provided by HQ and is off limits to Blue Cells and the Red Cell. Additional configuration specifics for the Gray Cell remote administration relay host are contained in the Network Specification document. Any restrictions or policies that detract from normal Gray Cell operations may result in score deductions.

2.4 Gray Cell may act as an "insider threat" to the BLUENET by performing actions as directed by the Gray Cell Team Lead. These actions may introduce malicious code to the host. This activity provides each Blue Cell the opportunity to detect, react and deter malicious activity. Blue Cell is permitted to deter threatening insider activity, but should keep in mind that applied mitigations that interfere with valid user tasks or automated traffic tools may result in various score deductions.

2.5 It is important to note that the Gray Cell is considered a "trusted insider". Gray Cell members, either deployed or remotely accessing the school enclaves, are not aware that their directed activity may be malicious or could cause harm to the BLUENETS.

2.6 Gray Cell actions will be accomplished on the designated Gray Cell workstations only. Gray Cell personnel must be provided access and be allowed to conduct these actions, as they are deemed consistent with behaviors of a traditional network user (e.g. email, web browsing, access to shares, etc.). Any lack of usability shall be reported to White Cell and may result in the loss of points. These actions may include, but are not limited to:

2.6.1 Sending/receiving email to/from any email address on the CDX network.

2.6.1.1 Ability to open attachments included in email.

2.6.1.2 Ability to click on links included in email.

2.6.2 Browsing the Web (CDX HQ, other BLUENET enclaves and SIMNET)

2.6.2.1 Scripting, .NET, ActiveX, Java and applets must be allowed to be enabled.

2.6.3 Downloading files from the Web (CDX HQ, other BLUENETs and SIMNET)

2.6.3.1 Includes HTTP/HTTPS and FTP.

2.6.4 Opening productivity files, Including MS/Open Office, text, images and PDFs.

2.6.4.1 Enabling of macros must be allowed.

2.6.5 Run preloaded applications and any software from the approved software list.

2.6.6 Run executable files downloaded/mailed from CDX HQ.

2.6.7 Navigate, access files, and create files on local file system.

3.0 Gray Cell Member Acknowledgement

I acknowledge that I have studied the *CDX 2016 Gray Cell Rules of Engagement*. Further, I understand that any failure to follow these instructions or the instructions of the CDX Leadership as it pertains to Gray Cell activities may have a serious and negative effect on CDX 2016 and may result in my early exit from the exercise.

Name (Last, First): _____

Organization: _____

Signature: _____

Date: _____