White Cell
Rules of Engagement
Version 3.0 Final

Purpose of this Document

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

Document Revision History

Version	Change Description	Change Owner	Date
1.0	FIRST DRAFT	2d Lt Frank Sclafani	13 Jan 2015
2.0	2015 FINAL VERSION	Angela Norwood	20 Mar 2015
3.0	2016 FINAL VERSION	Jim Titcomb	12 Feb 2016

1.0 White Cell Roles & Responsibilities

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

1.1. **Blue Cell Exercise Support**: White Cell serves to support the Blue Cells and ensure proper communication with CDX headquarters, timely delivery of CDX injects, resolution of concerns, and the understanding and compliance of the CDX directives.

1.2. **Enterprise Computer Network Defense Service Provider (CNDSP)**: White Cell will make operation order announcements (OPORD) for Common Vulnerabilities and Exposures (CVE)-styled items for which patches are to be applied or infrastructure updates are to be made. The announcements will usually follow a pre-determined timeline. However, out of band fragmentation orders (FRAGOs) may be required for infrastructure issues.

1.3. **White Cell Communications**: White Cell will communicate during the exercise in the manner outlined in the Communications Section of this document. White Cell will operate a digital announcement board and White Cell HQ will behave as the Network Operations Center (NOC).

1.4. **White Cell Tickets:** White Cell will manage the White Cell Ticket system that tracks any questions, incidents or problems. White Cell is responsible for managing the tickets through the process, communicating with appropriate Blue and Red Cells about ticket resolutions, and communicate with other White Cell members to ensure visibility of changes, issues, or decisions.

2.0 CDX 2016 White Cell Policy

2.1. White Cell members shall be fully versed in all the governing documented rules and shall be comfortable consulting with the documentation and CDX Headquarters staff.

2.2. The White Cell is to act as a customer service representative to Blue Cells. The White Cell is the main communication conduit to Blue Cells. The Blue Cell can ask any questions (about the exercise, scoring, injects, etc.) of the local White Cell member, who will work to answer.

2.3. White Cell members will not provide individual Blue Cells with privileged information including but not limited to: answers or support to the exercises, details about Red Cell operations, or information about other Blue Cell tactics and infrastructure. If CDX Leadership requests any additional information be provided to the Blue Cells during the exercise, the White Cell will ensure it is shared with all Blue Cell teams in a timely manner.

2.4. White Cell personnel will not reveal to the Blue Team any tactics, procedures, or vulnerabilities exploited by Red Cell against any other competitor Blue Team.

2.5. White Cell can assist the schools in working with the CDX engineering team to isolate technical problems, in order to identify them as CDX HQ (Headquarters) or school problems. If the technical issue is a Blue Cell originated problem, the schools are responsible for the final

troubleshooting and resolution of the problem without White Cell support. Any White Cell member identified as providing direct solutions to a Blue Cell originated problem will be violating the rules of engagement. White Cell impartialness is vital to the core of the CDX exercise.

2.6. Using the CDX ticket system, White Cell members shall document all Blue Cell or Red Cell activity that are counter to the directive and other governing documents. The White Cell member is responsible for gathering and documenting information, monitor the resolution of the ticket and report the findings back to the affected teams. The White Cell Team Lead and CDX Technical Lead will make all final rulings on score adjustments or penalties.

2.7. The results of the White Cell HQs decision will be posted at the appropriate time and the local White Cell representative will advise the affected teams.

2.8. If the Blue Cell is unsatisfied with a local White Cell member's answer to a question, comments, clarification of rules, the Blue Cell team may request the ticket be elevated to HQ White Cell.

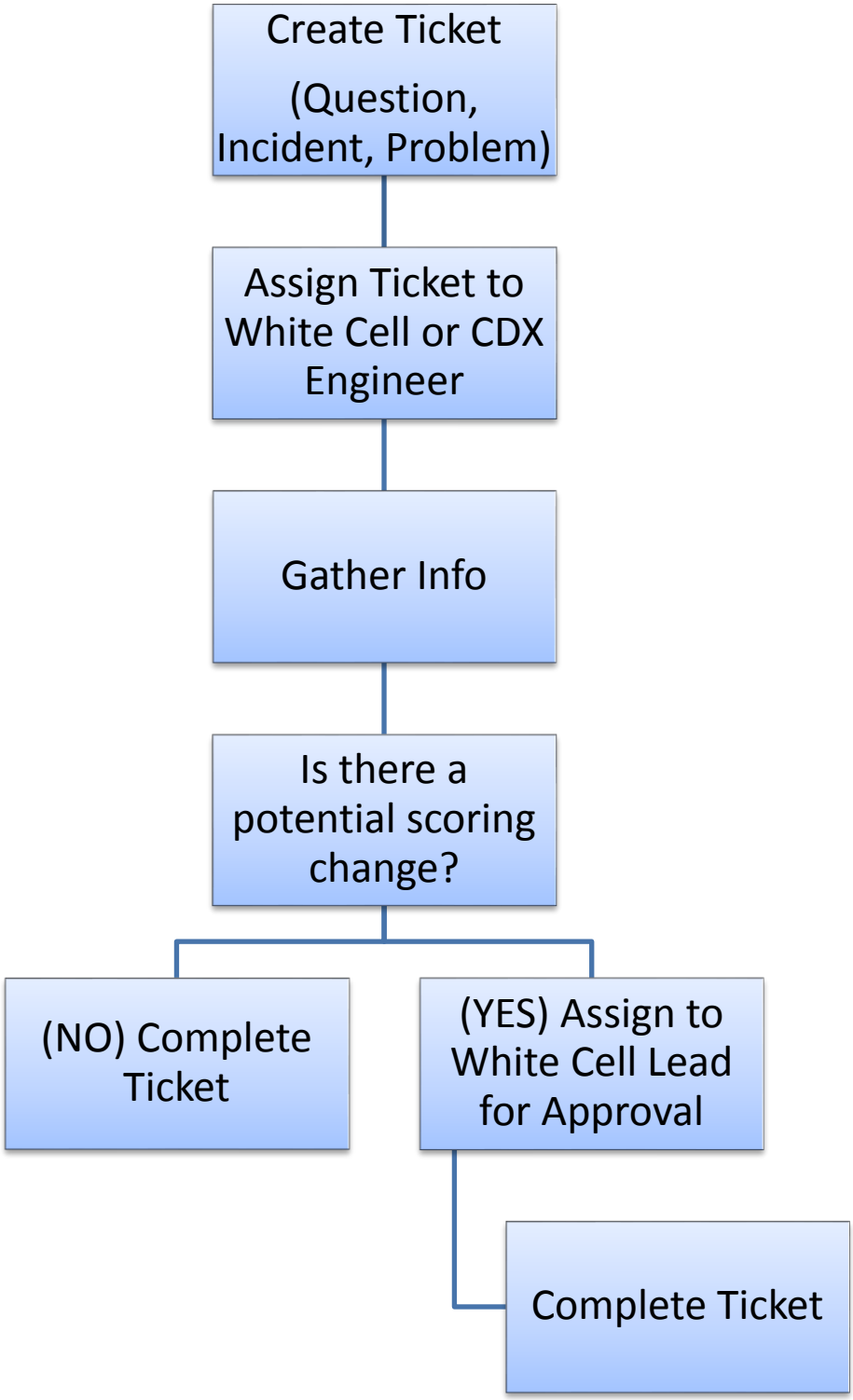
3.0 White Cell Problem Resolution Flow Chart

3.1. During business hours, any problems, concerns or official questions that are raised with the execution of the CDX exercise must be officially documented in a White Cell Problem ticket. Problem Tickets can be created by White Cell, Blue Cell, Red Cell, or CDX leadership and can encompass anything from exercise participant tactics, issues with infrastructure, concerns with CDX Directives or injects, or any other issues, questions or incidents within the CDX exercise.

3.2. During non-business hours, anyone can send an email or create a ticket for their White Cell member, who will respond at the start of the next business day.

3.3. White Cell reserves the right to make minor changes to the ticket process based on improving workflow or to better work within the ticket application itself.

3.4. Ticket System Process:



3.4.1. Local White Cell, HQ White Cell, Red Cell, Blue Cell or CDX Leadership members may create a White Cell ticket at any time. A ticket can be classified as a "Question", an "Incident" or a "Problem".

3.4.1.1. The ticket classification doesn't affect the workflow, but will help White Cell in managing the tickets.

3.4.1.2. Tickets can be created at any time by any team. However, White Cell will only work through and respond to tickets during White Cell work hours.

3.4.2. Once a ticket is created, it is assigned to a Local White Cell member. The ticket can be reassigned to a HQ White Cell Member if it requires HQ investigation.

3.4.2.1. Whoever is assigned a ticket is responsible for working the ticket through to completion.

3.4.2.2. There is no stated timeline to completed tickets, but a ticket assigned to a White Cell member is their top priority.

3.4.2.3. If a Blue Cell creates the ticket, the Local White Cell member assigned to that Blue Cell will ensure that the ticket is being worked and is answered satisfactorily. Even if the ticket is reassigned to HQ.

3.4.3. The person assigned the ticket, most likely a White Cell member, is responsible for gathering the necessary information to answer the ticket satisfactorily.

3.4.4. If there is a potential scoring adjustment, then the scoring adjustment will always be approved by CDX White Cell Lead and the CDX Technical Lead.

3.4.5. Any decisions, answers to questions, or scoring adjustments will be detailed in the "Decisions" section of the ticket.

3.4.6. CDX documents or other White Cell tickets that are used in the decision or resolution of a ticket will be documented in the "Reference" section of the ticket.

3.4.7. If a ticket is created or related to Blue Cell or Red Cell, then the assigned White Cell person will add them to the "cc" group if the ticket does not contain proprietary information.

3.4.7.1. It is the responsibility of the White Cell to ensure that tickets cc'd to Blue Cell or Red Cell do not contain information that they should not be privy to. This includes but is not limited to information about other teams, details of scoring decisions before decision is announced, or information about future injects.

3.4.8. When a ticket is resolved, the White Cell will be responsible for communicating to the ticket creator the details of the ticket decision.

3.4.9. If a ticket has information that all White Cell members should be privy to, then the White Cell ticket owner will communicate that information to all White Cell members.

3.4.9.1. White Cell should continuously look at the tickets so they can track what is going on across the game.

3.5. **White Cell Announcement Board**: White Cell will maintain a WordPress webpage that will be accessible to all teams. This webpage will act as a communications board where posted announcements include but are not limited to: Gray Cell status (on/off duty), start of business day, OPORDs, rules, outages and injects. The announcement board will also be used to CDX decisions throughout the exercise.

3.5.1. **Simulate OPORD (Operational Orders)**: White Cell will make announcements (OPORD) for CVE-styled items for which patches are to be applied. The announcements will follow a pre-determined timeline.

3.5.2. **White Cell Injects:** During the exercise, the White Cell may provide Blue Cells with "injects" with little to no warning. These injects are designed to simulate additions or changes to the Blue Cell infrastructure. The injects will be posted on the WordPress board. Local White Cell may also alert Blue Cell when the posts are made, but it is the responsibility of Blue Cell to monitor the WordPress board.

3.6. **Local to HQ Communications**: For the 2016 CDX there will be two White Cell representatives per Blue Cell team. The Local White Cell representatives will be physically located with each Blue Cell team. The HQ White Cell representative will be physically located at CDX HQ in Maryland. The role of the Local White Cell representatives is to act as the on-site customer service representative and act as a liaison with their counterpart back at HQ. The role of the HQ White Cell representative is to facilitate the communications with their designated Blue Cell team and with their Local White Cell counterpart. The HQ White Cell representative will also consolidate and prioritize communications to be passed up to the White Cell Lead.

3.6.1. The Local White Cell members and the HQ White Cell will be in constant communication during the CDX. The main method of communication within the White Cell will be through the White Cell Chat System. A jabber server will be set up to facilitate the chat. Using jabber will make it quick and easy to talk to anyone on White Cell, allow other White Cell members see decisions and stay abreast of issues. The jabber server will also log the chats for recall if necessary.

3.6.2. Each White Cell will also have a phone number and access to a phone at their duty station.

3.6.3. During off hours, the Local White Cell and the White Cell Leads will be available by phone if there is an emergency.

4.0 White Cell Member Acknowledgement

I acknowledge that I have studied the CDX 2016 White 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 White 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: _____