CyberPatriot IV

The National Finals Competition
Competitors' Guide

March 22 - March 24, 2012
National Harbor, Maryland

"Have <u>you</u> got what it takes?"

Presenting Sponsor:

NORTHROP GRUMMAN
Foundation

CyberPatriot Program Office
Air Force Association
1501 Lee Highway
Virginia 22209-1198

March 1, 2012

Dear CyberPatriot Competitors,

Congratulations on qualifying for the CyberPatriot National Finals Competition. Hundreds of teams began, but only a few remain among the elite field competing for the prestigious Open Division's President's Cup and the All Service Division's Commander-in-Chief's Cup.

You have worked hard to get here, you have thrived under pressure, and you have shown that you have what it takes to win in a highly technical competition. But so have several other teams, and now the competition will become even more difficult, as we work to identify the one best team in each division.

What follows are instructions regarding your visit to the Washington, DC area, as well as the technical and administrative aspects of the competition you need to understand.

I encourage you to read this document as a team page-by-page to ensure every member of your team has a complete understanding of what you can expect and what will be expected of you during your visit and on the competition floor. Some of it you will have seen before, but you need to understand all of it, so please read this document carefully.

We have done everything we can to provide clear guidance and to ensure a fair competition. If anything is unclear, I encourage you to let us know immediately. Contact our Director of Competition Operations, Frank Zaborowski, at 703-247-5840 or via email: f.zaborowski@uscyberpatriot.org with any concerns or requests for clarification.

Best of luck.

Sincerely,

Bernie Skoch

Bernie Skoch
CyberPatriot Commissioner

SECTION A. Logistics and Planning

Table of Contents

POC: Rachel Zimmerman (unless otherwise specified)
R.zimmerman@uscyberpatriot.org, 703-247-5834

The following items should be reviewed with team members, coaches, and any other members of your team's traveling party. Questions may be directed to the points of contact indicated.

1. **<u>Protocol</u>**

   <u>Open Division teams</u>. Though members of the Open Division are not expected to observe military courtesies, we ask that competitors conduct themselves in a respectful and deferential manner when distinguished visitors are present in the competition area. Referees and CyberPatriot staff will ensure that visitors to the competition area do not distract competitors.

   <u>All Service Division teams</u>. General officers, government officials and executives from industry will be visiting the competition. When not in competition periods, cadets should extend all appropriate military courtesies. While participating in competition periods, cadets should continue their work as if the visitors were not present. All visitors will be asked to avoid distracting competitors and will be advised that cadets in competition periods will not be called to attention. Cadets may expect distinguished visitors to greet them and to engage with them. Cadets should reply directly and respectfully. Green Team members and CyberPatriot staff will monitor these visits, and will respectfully remind visitors of our non-interference policy as necessary.

   Point of Contact (POC): Bernie Skoch, b.skoch@uscyberpatriot.org, cell: 479-530-8568.

2. **<u>Airport Arrival</u>. Individual ground transportation will be arranged in the near future and emailed to coaches directly.**
   Driving and Parking: For teams that are driving to the competition, your destination is the Gaylord National Resort and Convention Center, 201 Waterfront Street, National Harbor, Maryland 20745. Complete by-origin driving directions can be found here: http://www.gaylordhotels.com/gaylord-national/directions-transportation/#map

   You will need to park your vehicle in the Gaylord's self parking garage. Upon check-in, tell the front desk agent that you have a vehicle. Please make sure that the vehicle charges are placed on the coach's sleeping room so we can have those charges covered appropriately.

3. **<u>Registration and Arrival</u>.** Your team's first stop at the Gaylord National Resort should be the hotel registration desk where you will receive room assignments and keys. We will have pre-registered your team with the hotel. A member of the CyberPatriot staff will be present near the hotel registration desk to greet and assist you if you have any questions. Additionally, the CyberPatriot staff member will have a CyberPatriot Welcome Packet for each team that will contain each team's meal vouchers and badges. If your team is delayed en route, please advise the CyberPatriot Program Office as soon as possible by calling Bernie Skoch, cell: 479-530-8568.

4. **<u>Lodging Expenses</u>.** AFA will cover lodging expenses for Open Division teams; Canadian and All Service Division teams should check with their respective headquarters to verify what method of payment will be used. At check-in, the hotel will request a credit card from each team's coach against which to charge incidental expenses (in-room telephone calls, in-room Internet use, movies, etc.). Coaches are responsible for any such incidental charges and for room damages.

5. **Checked Baggage.** AFA will reimburse Open Division teams for the cost of one piece of checked baggage per team member on the flights to and from Washington, D.C. (six students and two adults, for a total of eight pieces of checked baggage per team). All Service Division Teams, please check with your Headquarters as to how baggage will be handled.

6. **Meals.** AFA will provide all meals (either in-kind or by voucher) between Wednesday evening and Sunday morning, for the six competitors and two adults of each team*. Complete information on the locations and times of meals will be supplied upon arrival.

   * Please note: Any additional team personnel (outside of the six competitors and two adults) that wish to attend the Friday awards banquet must register and purchase tickets from AFA.

7. **Attire.** During the Equipment Familiarization and Competitor's Dinner on Thursday, all competitors should wear their teal CyberPatriot t-shirts* with slacks (jeans are discouraged). During competition on Friday, All Service Division teams should wear their short sleeved duty uniform without a tie; Open Division teams should wear their CyberPatriot teal t-shirts* with slacks (jeans are discouraged). During the CyberPatriot Awards Ceremony, All Service Division teams should wear their Service Dress (Class "A") uniform or equivalent business attire for coaches and other adults. Open Division male competitors should wear coat and tie; female competitors should wear a knee-length (or greater) skirt or slacks, and blouse. Coaches and other adults should wear equivalent business attire. For the tour on Saturday, all competitors should wear their teal CyberPatriot t-shirts*.

   * Please only wear the CyberPatriot-issued National Finals Competition teal t-shirts. Some teams may have made their own CyberPatriot t-shirts, however these should not be worn in lieu of the teal CyberPatriot t-shirts.

8. **Media Information**. Media coverage is important to the growth of CyberPatriot and is a great opportunity to showcase the success of your teams. We want to make it as easy as possible for the media to cover the competition. You can review the CyberPatriot Media Guidelines at the following URL: http://www.uscyberpatriot.org/about/Pages/OtherMediaInformation.aspx

   Media Preparations. Advise your team that there may be photographers and a camera crew present during competition. The photographers and camera crew have been briefed on the competition's non-interference policy. If coaches believe photographers and/or camera crew are creating a distraction, they should advise a member of the Green Team or a member of the CyberPatriot staff immediately.

   If an interview is requested by the media:

   - If possible, notify the CyberPatriot media coordinator, Merri Shaffer. She can be reached before the competition at 703-247-5847 (office), or during the competition at 615-830-3134 (cell).
   - Articulate to all members of your team that this is a "friendly" competition and that no disparaging remarks will be made about other teams.
   - Foul or crude language is prohibited.

   Official Announcements

   There will be an official press release announcing the winners of each division by Monday, March 26. We will also provide coaches with a template press release to be forwarded to home town publications.

9. **Competition Space.** If your team would like to bring anything to display in your team's competition space, please submit a written request to r.zimmerman@uscyberpatriot.org stating what you would like to bring, the dimensions of the item, and how you would like it displayed. Only approved items will be allowed in the competition area. Please note that, due to agreements with CyberPatriot National Sponsors, only National Sponsor's logos may be displayed in the Competition Space.
   - Please note that while teams are allowed to bring printed reference materials for use during competition, CyberPatriot does not provide printers for attendees of the National Finals Competition. The Gaylord National Resort has a business center onsite for minor printing needs, but teams are responsible for the associated costs.

10. **If Your Team Wins Your Division:**

- CyberPatriot requests interviews with the winning teams from each division immediately following the Awards Banquet on Friday, March 23. A camera crew will be filming the Finals round and CyberPatriot will use this footage to produce materials that will illustrate the impact of the program.
- The winning teams from each Division (and their mentors and coaches) should report for an interview following the Awards Banquet. The exact location and time of this interview will be included in the updated schedule you will receive upon arrival at the Gaylord.

11. Schedule

The schedule below is tentative. A finalized schedule will be emailed to coaches one week prior to the event. It is essential that your team be on time for all events. Your team is one of 26 that will be competing at the National Finals Competition. We cannot hold the start of any events for a team that is late in arriving.

Wednesday

Teams arrive
Dinner is done by voucher for teams

Thursday

Time	Activity	Who	Location	Dress
Breakfast	Voucher	Both Divisions		
8:00 – 8:45	Opening Ceremonies	Both Divisions	Maryland C/D	CyberPatriot T-shirts and slacks
9:00 – 12:00	Equipment Familiarization	Open Division	Maryland B/4/5/6	CyberPatriot T-shirts and slacks
9:00-10:45	Mentoring Moments	All Service Division	Maryland A	CyberPatriot T-shirts and slacks
Lunch	Voucher	Both Divisions		
1:00 – 4:00	Equipment Familiarization	All Service Division	Maryland B/4/5/6	CyberPatriot T-shirts and slacks
4:00-5:45	Mentoring Moments	Open Division	Maryland A	CyberPatriot T-shirts and slacks
6:00 – 8:00	Competitors' Dinner with Northrop Grumman Mentors	Both Divisions	TBD	CyberPatriot T-shirts and slacks

Friday

Time	Activity	Who	Location	Dress
6:45 – 8:00*	Continental Breakfast*	Both Divisions	Maryland B/4/5/6& Competitors' Lounge*	
7:30 – 12:30	Competition Period	Open Division	Maryland B/4/5/6	CyberPatriot T-shirts and slacks
7:30 – 11:15	Forensics Competition	All Service Division	Maryland B/4/5/6	Duty uniforms (without tie)
11:30-1:00	Lunch	Both Divisions	Maryland Foyer	
1:30-6:30	Competition Period	All Service Division	Maryland B/4/5/6	Duty uniforms (without tie)
2:00-6:15	Forensics Competition	Open Division	Maryland B/4/5/6	CyberPatriot T-shirts and slacks
3:00-4:00	Coaches Forum	All coaches	Competitors' Lounge	
7:30	CyberFutures Banquet featuring CyberPatriot Awards	Both Divisions	Maryland CD	Refer to section A-7

Saturday

Time	Activity	Who	Dress
Breakfast	Voucher		
	Tour of Northrop Grumman facility	Both Divisions	CyberPatriot T-shirts and slacks
	Tour continue to Pentagon Memorial, Air Force Memorial	Both Divisions	CyberPatriot T-shirts and slacks

We are still finalizing the times for the Northrop Grumman facility tour. We are aiming for a 10 a.m. tour.

12. **Coaches' Forum**. The CyberPatriot Team Coaches Forum will be held at 3:00 – 4:00 pm on Friday, March 23, in the Competitors' Lounge. Mentors may attend. Please submit agenda items to the Director of Competition Operations, Frank Zaborowski, no later than March 15, 2012.

POC: Frank Zaborowski, f.zaborowski@uscyberpatriot.org.

13. CyberPatriot Program Office Staff. During your stay at The National Finals Competition, the CyberPatriot Program Office staff will be ready to assist you. The members of the staff are:

Eric Danner	Manager, Competition Systems
Laine Martens	Program Manager and Outreach Coordinator
Bernie Skoch	Commissioner, CyberPatriot Program
Frank Zaborowski	Director of Competition Operations
Rachel Zimmerman	Manager, Competition Events and Communications

14. Competitor Protection. The safety of our competitors is a top priority for the CyberPatriot program. Coaches and chaperones are expected to account for their team members at all times. If a competitor, even if they are 18 years of age, is missing, injured, hospitalized, or a victim of a crime, the coach or chaperone shall notify the CyberPatriot Program Office staff immediately.

SECTION B. Competition Organization and Administration

Table of Contents

Paragraph

POC: Frank Zaborowski
F.zaborowski@uscyberpatriot.org, 703-247-5840

1. Competition Overview

The CyberPatriot IV National Finals Competition consists of 24 U.S. teams and two Canadian Teams competing in the following two events:

- **Network Security Competition** -- *powered by the Cyber Network Exercise System (CyberNEXS)*

- **Forensics Competition** -- *conducted with the Department of Defense Cyber Crime Center (DC3) Crime Scene Forensics Challenge*

The U.S. teams will compete against each other in the All Service and Open Divisions. Canadian teams will compete in the International Exhibition, which will occur at the same time as the Open Division.

The competition events are executed by division in time blocks. Time blocks are assigned to divisions and, when required, time slots are assigned to teams within a time block. The Network Security competition is a competition in which teams in their respective division compete for five consecutive hours in one time block. The DC3 Crime Scene Forensics Challenge is a 30-minute team event in which teams are assigned specific 30-minute time slots to compete within their division's time block.

2. Competition Organization

The organization for the CyberPatriot IV National Finals Competition consists of the CyberPatriot Program Office, competitor teams, competition administration teams, and the support staff. The following are the groupings, roles and responsibilities of the CyberPatriot Program Office and the teams. (See Figure B-1.)

a. Personnel Groupings

(1) Competitors. Competitors is a grouping of all participants competing in the competition.

(2) Competitor Team. A Competitor Team is a grouping of the participant teams competing in the competition. Blue Teams and competitor teams are synonymous.

(3) Competition Administration Team. Competition Administration Teams facilitate, operate, and administer competition events. Green, White, Red, and Forensics Teams are competition administration teams. The Competition Administration Teams are headed by Team Captains.

(4) Competition Staff. Competition Staff is a grouping that includes all members of the CyberPatriot Program Office staff, members of the competition administration teams (Green, Red, White, and Forensics), and any other support staff.

b. CyberPatriot Program Office. The CyberPatriot Program Office is responsible for the administration, logistics, and conduct of the CyberPatriot IV National Finals Competition. The following personnel will be involved in the competition.

(1) Commissioner, CyberPatriot Program. The Commissioner has overall responsibility for the National Finals Competition and is the decision authority for the competition. Any issue that has not been delegated to another authority, to include scoring issues, is exclusively within the scope of Commissioner's decision authority.

(2) Director of Competition Operations. The Director of Competition Operations is responsible to the Commissioner for the conduct and oversight of the competition, and is the direct interface between the competition teams and the Commissioner. Based on the advice of the appropriate competition administration teams (Green, White, Red, and Forensics), the Director of Competition Operations will make recommendations to the Commissioner on competition issues for the Commissioner's consideration.

(3) Manager, Competition Systems. The Manager, Competition Systems is responsible for the setup, operation, and coordination of all electronic systems that support the competition. Additionally, the Manager, Competition Systems will assist the Director of Competition Operations with oversight of the competition.

c. Blue Teams (Competitors)

(1) The Blue Teams are the student competitor teams in the Open and All Service Divisions, and the International Exhibition. Each team shall consist of no more than five members. Blue Team members wear teal colored T-shirts.

(2) Each team may have one coach and one mentor/chaperone present at the competition – they may be faculty/staff members of the school or unit sponsors. Neither the coach nor the mentor may assist or advise the team during the competition.

(3) All competitors shall wear badges identifying team affiliation at all times during the competition.

(4) Team Captain. Each team shall designate a Team Captain for the duration of the competition to act as the liaison between the competition staff and their team before and during the competition.

d. Green Team

(1) Referees. The Green Team will monitor the Blue Teams' performance and conduct. Blue Team Captains will contact the Green team with questions or issues, during the Network Security and Forensics Competitions. Green Team members will then either resolve the issues or questions or escalate them as necessary to the Director of Competition Operations. Cases that involve addition or deduction of points, or disqualification of individuals or teams, will be escalated to the Director of Competition Operations for further resolution. Rulings made by the Commissioner, CyberPatriot program are final. Green Team members wear green polo shirts.

(2) Visitor Control. The Green Team will monitor guest/VIP visits to the competitors' spaces.

(3) Competitor Lists. The Green Team will maintain the official lists of competitors, coaches, and chaperones and contact information for competition personnel.

(4) Competitor Movement Control. The Green Team will control the movement of competitors in and out of the competition area.

e. White Team

(1) Policy Enforcer. The White Team is the policy enforcer of the Network Security Competition. While the CyberPatriot Commissioner sets up and defines how the competition will be run, the White Team acts as managers of Blue Team scenarios. The White Team will ensure that the exercise is run fairly and that each Blue Team participant is monitored, supported, and scored within the rules of the competition as dictated by the Commissioner**.** White Team members wear white shirts.

(2) Maintenance. Throughout the competition, White Team members will be responsible for maintaining the competition equipment and can troubleshoot systems that malfunction when the malfunction is not part of the competition itself.

(3) White Team members are also responsible for judging functions during the Network Security Competition.

f. Red Team

(1) Aggressor. The Red Team is the aggressor of the Network Security Competition. Red Team activity subjects competitors to the real-world dilemma of implementing security to meet best practices, balanced with the need to offer services in a timely and efficient manner. Red Team members wear red shirts.

(2) Assessment. The purpose of the Red Team is to conduct an assessment and attack on the network environment being secured by the Blue Team within the rules of the competition. The Red Team launches automated or manually crafted attacks against Blue Team systems. The Red Team rates a given attack's success, which has a direct effect on the competition's final outcome. In essence, the Red Team simulates real world attacks by employing the same tactics used by hackers.

g. Forensics Team. The Forensics Team is a competition administration team responsible for the administration of the Forensics Competition. The team will administer and score the Forensics Competition. Forensic Team members wear blue polo shirts.

h. Support Staff. The Support Staff are personnel who are members of or under the cognizance of the CyberPatriot Program Office, who provide support to the competition, but do not directly participate in the competition or its functions. Docents (guides), door monitors, etc. are examples of the Support Staff.

3. Competition Area

The National Finals Competition will take place in the Competition Area. The area has designated spaces for the functions of the competition. No one except Blue Team members and the competition staff may enter the competition spaces without permission of the Green Team. Unauthorized personnel in the competition spaces could result in disqualification of a team. The following is a breakdown of the Competition Area.

a. Network Security Competition Spaces. In the competition area, 14 competition spaces will be designated for the Network Security Competition. Teams will be assigned to specific competition spaces for their division's competition time block and team time slots, during the equipment familiarization period. The International Exhibition will use the Open Division's competition time block. The areas will contain:

- Table
- 5 Chairs
- 5 laptop computers
- 32 inch monitor
- 8 port hub
- Easel with large pad of paper
- Category 5, Unshielded Twisted Pair Cable

b. Forensics Competition Spaces. Additionally, two spaces will be designated for the Forensics Competition. The spaces will be used for the 30-minute competition time slots assigned to teams for the Forensic Competition. The spaces will contain a simulated crime scene and an evidence work area.

c. Competition Administration Spaces. The competition administration spaces include the competition administration teams' areas and the CyberPatriot Program Office. The competition administration spaces are off-limits to competitors, with the exception of the Green Team area.

d. Competitors' Lounge. The competitors' lounge is a break area designated for competitors, coaches, mentors, and the competition staff. Refreshments are available in the competitors' lounge for competition personnel.

e. Spectator Area. The spectator area will be designated for personnel not competing to view the competition spaces. Spectators are not permitted to communicate with the competitors in the competition area (to include cheering and words of encouragement).

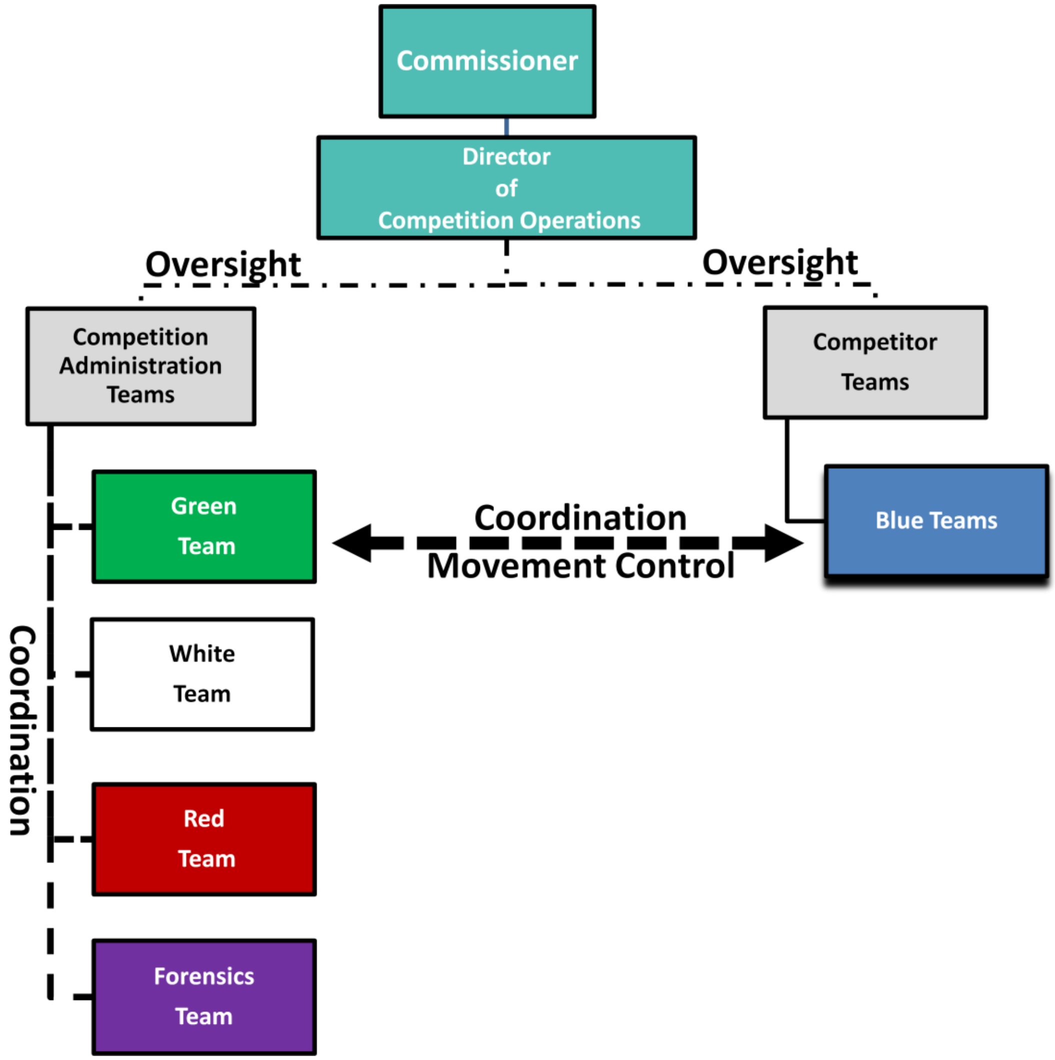


Figure B-1. Competition Administration Relationships

4. General Competition Rules

a. Purpose and Rules. The CyberPatriot program operates under the premise that that all competitors and coaches conduct themselves with the highest integrity. To prevent the perception of misconduct that would jeopardize the integrity of the competition and to avoid friction between teams, the following rules have been established for the National Finals Competition.

(1) Team Captains are encouraged to work with the competition staff to resolve any questions or disputes regarding the rules of the competition or scoring methods before the competition begins.

(2) Protests by any Blue Team members will be presented by the Blue Team Captain to the Green Team as soon as possible. The Green Team will attempt to settle any protests or questions arising before, during, or after the competition. Cases that involve addition or deduction of points, or disqualification of individuals or teams, will be escalated to the Director of Competition Operations, who will make a recommendation on further action to the Commissioner, CyberPatriot Program. Rulings by the Commissioner are final.

(3) Blue Teams shall compete with no outside assistance or communication, to include coaches, mentors, chaperones, or other guests in the competition area. Except in the case of an emergency, the prohibition on communication includes when a competitor leaves the competition area for any non-emergency reason, to include use of the restroom.

(4) No unauthorized personnel are allowed in the competition spaces.

(5) No changes shall to be made to laptops or other competition hardware (e.g., hubs, cable, etc.) or software that may adversely affect other users of that system.

(6) Electronics: No PDAs, memory sticks, CDROMs, electronic media, or other similar electronic devices are allowed in the competition area during the competition, unless specifically authorized by the competition administration teams or the CyberPatriot Program Office.

(7) Cell phones are prohibited in the competition area (except in case of emergency). Competitors may not use cell phones during their division's competition or International Exhibition's time block or team's competition time slot.

(8) All competitors shall wear their badges when in the competition area.

(9) Competitors shall not conduct offensive activity against the White Team, other Blue Teams, or the Red Team or competition or non-competition systems.

b. Penalties. Reported violations of the competition rules will be investigated. Confirmation of a rule violation may result in disqualification of an individual or team or a competition penalty (e.g., points, time, etc.) against the team, as determined by the Commissioner, CyberPatriot Program.

(1) Individual Disqualification. In the event of an individual disqualification, that team member must leave the competition area immediately and must not re-enter the competition area at any time. Disqualified

individuals are ineligible for team trophies, scholarships, or any other recognition by the CyberPatriot Program Office. Replacement of a disqualified team member is at the sole discretion of the Commissioner, CyberPatriot Program.

(2) Team Disqualification. In the event of a team disqualification, the entire team must leave the competition area immediately and is ineligible for any team award.

c. Rules Questions. If you have questions concerning the rules or the conduct of the competition, please contact the Green Team or the CyberPatriot Program Office.

5. Scoring

The National Finals Competition and the International Exhibition scores will be an aggregate of each team's performance in the Network Security and Forensics Competitions. The Network Security Competition will account for **90%** of each team's overall score, and the Forensics Competition will account for **10%** of the overall score.

The National Finals Competition winners will be selected according to the highest overall team score at the end of the competition within each division and the International Exhibition.

Scores will not be released by the Competition Staff, during the competition.

a. Network Security Competition (powered by CyberNEXS) Scoring Criteria

(1) Defense Criteria

(a) Success in maintaining critical services adds percentage points
(b) Success in removing vulnerabilities adds percentage points
(c) Successful attack on Blue Teams by the Red Team deducts percentage points

(2) Trouble Ticket Criteria**.** Trouble Tickets (TT) are a critical aspect of cyber defense. The timeliness and completeness of the ticket will add to the team's score. The value of the TT is related to the detail with which it is written. The following list is a hierarchy of detail starting with the minimal TT score, progressing to a maximum TT score.

(a) Notices a problem, but doesn't have much detail
(b) Notices a problem, shows IDS or system logs confirming problem
(c) Identifies problem, and details description of fix
(d) Fixes problem, and details system re-configuration
(e) Detects attacker, identifies and fixes problem, provides complete details

b. Forensics Competition Scoring Criteria

(1) Scores will be expressed as a number between 0 and 100.

(2) Each piece of evidence will have a unique score associated with it.

(3) Please see Section D for complete information on Forensics Competition scoring.

c. Score Reset. (See Section C, paragraph 4.) In the event of a network outage, all Network Security Competition scores may be reset. It is critical that competitors take notes of their actions during the competition to avoid wasted time after a score reset.

d. General Scoring Notes

(1) The top three teams with the highest overall scores from each Division will be recognized at the Awards Banquet following the competition.

(2) The teams from each Division with the highest score in the Forensics component will be recognized at the Awards Banquet.

(3) Network Security Competition scores will be maintained by the White Team, but will not be shared with competitors until after the end of the competition. There will be no running totals provided during the competition.

(4) Any team that tampers with or interferes with the scoring system (ScoreBot) or with another team will be disqualified.

(5) Students will be evaluated in two ways during Network Security Competition: quantitatively and qualitatively. These methods will apply both objective (automated scoring of vulnerabilities or services availability) and subjective (quality and timeliness of trouble tickets). This method includes straightforward criteria for assessing points and will be used by the White team to uniformly judge the quality of the Blue Team communications.

e. Scoring Issues, Penalties, and Assessments. If an issue arises where points may be added to, or subtracted from, a team’s score through a penalty or assessment, the appropriate Competition Administration Team Captain will advise the Director of Competition Operations on potential courses of action. The Director of Competition Operations will then make a recommendation to the Commissioner, CyberPatriot Program, who will render a final decision on the penalty or assessment.

6. Blue Team Substitution Procedures

When a competitor can no longer compete, due to a medical issue or emergency, ***only*** the Alternate Blue Team Member may be substituted for a primary Blue Team member. All substitutions will be controlled by the Green Team. Under no circumstances may a substitution be made, without the approval of the Green Team. Once a Blue Team coach has made a substitution, the team may not make another substitution.

a. Reasons for Substitution. Medical issues and emergencies are the only reasons for replacing a primary team member with the Alternate Blue Team Member.

b. Substitution Procedures. The Green Team is the central authority for all substitutions. The respective team's coach and the Green Team shall be involved in all substitutions. Substitutes shall be the Alternate Blue Team Member on the team's official list, held by the Green Team. The following are the substitution procedures:

(1) In the Competition Area

(a) Blue Team Captain**.** The Blue Team captain will notify the Green Team of a competitor with a medical issue or an emergency who must permanently leave the competition and requires the Alternate Blue Team Member to replace the competitor.

(b) Green Team. Upon notification by the Blue Team Captain that a substitution is required for their team, the Green Team will contact the respective coach and inform the coach of the situation.

(c) Coach. The coach will notify the Green Team of the name of the Alternate Blue Team Member who will substitute for the primary team member.

(d) Green Team. The Green Team will verify the Alternate Blue Team Member's name, log the substitution, and notify the Director of Competition Operations of the substitution.

(2) Outside the Competition Area

(a) Coach. The coach will notify the Green Team of the primary team member, with a medical issue or emergency, who will be replaced and the name of the alternate team member who will substitute for the primary team member.

(b) Green Team. The Green Team will log the substitution and notify the Director of Competition Operations of the substitution.

(3) Disputes. In the event of a dispute concerning the validity of a substitution, the Green Team will immediately notify the Director of Competition Operations of the situation.

7. Commissioner's Critical Information Requirements

The Commissioner, CyberPatriot Program requires certain information to safely and effectively conduct the National Finals Competition. The Commissioner shall be notified by the competition staff or coach/chaperone if the following events occur:

a. Network Security Competition system (CyberNEXS) outage of more than 10 minutes

b. Missing competitor

c. Injured competitor requiring hospitalization

d. Criminal act against a competitor, coach, chaperone, mentor, competition staff, or CyberPatriot

supporter

e. **Violation of competition rules that involve penalties or disqualification of a team member or team**

f. **Severe weather or natural disaster that could negatively affect the competitors or competition**

SECTION C. Network Security Competition

Table of Contents

Paragraph

POC: Eric Danner
E.danner@uscyberpatriot.org, 703-247-5807

1. Network Security Competition Overview

The Network Security Competition is powered by CyberNEXS and operated by Scientific Applications International Corporation (SAIC). Each division will have a five-hour time block to compete. The International Exhibition will compete with the Open Division. The main differences between the in-person Network Security Competition and the first three rounds of CyberPatriot IV are the:

- Competition is in-person.
- Competitors use up to 12 virtual images vice one or two images.
- SAIC-led Red Team will launch attacks against Blue Team systems.
- White Team judges Blue Team responses.
- Blue Team Captain is the point of contact for the Blue Team.
- Green Team is the competition staff point of contact for the Blue Team.

In the Network Security Competition scenario, the Blue Team is filling recently hired administrator positions and is assuming responsibility for each of their systems.

2. Network Security Competition Rules

a. Competition Systems

(1) All Blue Teams will start the competition with identical systems configured with dual-boot partitions (each of which is intended for a specific Division). Teams are **NOT** to make any type of changes to the configuration of the host machine. Any changes made to the host machine that adversely affect other users of that system may result in immediate disqualification of the entire team in question. If you are unsure if a given change is acceptable, contact a member of the Green Team **beforehand**.

(2) Examples of prohibited conduct in the above context could include, but are not limited to, deleting or reconfiguring a drive partition, making changes to the system's BIOS, changing user permissions on the host machine, etc.

(3) Teams may not remove any computer, networking device, or other peripheral from the competition area.

(4) All teams will be connected to the CyberNEXS central scoring system.

(5) Teams must not connect to any devices or peripherals that are outside the competition network.

(6) Teams may not modify the hardware configurations of competition systems. Teams must not open the case of any server, printer, PC, monitor, KVM, router, switch, firewall, or any other piece of equipment used during the competition. All hardware related questions and issues should be referred to the Green Team.

(7) Teams should not assume any competition system is properly functioning or secure.

b. Competition Play

(1) During the competition, team members are forbidden from entering or attempting to enter another team's competition workspace.

(2) Teams must compete without outside assistance from non-team members which includes team coaches and mentors/chaperones.

(3) Electronics: No PDAs, memory sticks, CDROMs, electronic media, or other similar electronic devices are allowed in the room during the competition unless specifically authorized by the White Team in advance.

(4) Cell phones are prohibited in the competition area (except in case of emergency).

(5) Each Blue Team computer will come pre-loaded with Snort, an intrusion detection system (IDS), and BASE (Basic Analysis and Security Engine), a network monitoring utility.

(6) Printed reference materials (books, magazines, checklists) are permitted in competition areas and teams may bring printed reference materials to the competition (Please note that there will be no printer available onsite for Blue Team use.)~~.~~

(7) Team sponsors, observers, and team alternates are not competitors and are prohibited from directly assisting any competitor through direct advice, "suggestions," or hands-on assistance. Any team sponsor or observers found assisting a team will be asked to leave the competition area for the duration of the competition and a penalty (up to and including disqualification of the entire team) will be assessed against the team.

(8) Team members will not initiate any contact with members of the Red Team during the hours of live competition.

(9) On occasion, Green Team members (referees) and CyberPatriot staff may escort individuals (VIPs, press, etc.) through the competition area.

(10) Teams are free to examine their own systems, but no offensive activity against the White Team, other Blue Teams, or the Red Team will be tolerated. This includes port scans, unauthorized connection attempts, vulnerability scans, etc. Any team performing offensive activity against other Blue Teams, the White Team or the Red Team will be immediately disqualified from the competition. If there are any questions or concerns during the competition about whether or not specific actions can be considered offensive in nature, contact the Green Team before performing those actions.

(11) Blue Team Responsibilities

(a) Maintain the target systems and network defenses

(b) Review initial system configurations to verify that machines are properly configured and patched against vulnerabilities

(c) Manage network and host-based systems to counter any active threat

(d) Report computer misuse to competition staff

(e) NOT modifying in any way users named:

(1) "CNDXAdmin;"
(2) "CNDXUser;"
(3) "CNDXAdm;"
(4) "CyberNEXSAdmin;"
(5) "CyberNEXSUser;" and,
(6) "CyberNEXSAdm."

These accounts are used for administration purposes and are not used to gain Red Team access to competitors' systems.

(f) Allow ICMP (ping) within the internal network and to external devices, other than the firewall.

(12) The main priorities at hand are availability and security. Teams should do whatever is necessary to achieve security on their network without denying services to legitimate users.

3. CyberNEXS System Description

a. Blue Team Systems: The basic competition network will consist of:

(1) Servers: CentOS, Debian, Ubuntu, Windows 2003, Windows 2008,
Workstations: Fedora Linux, Linux Mint, Windows 7, Windows XP, Windows Vista
(See Figure C-1 – CyberNEXS Network.)

(2) Network Devices such as dedicated firewalls

(3) One laptop on the SysAdmin network will be dedicated and manned to display the System Status Board. (See Figure C-1 – CyberNEXS Network for an example of the interface the Blue Teams will use during the exercise.) This will be projected on the external monitor at the team's workstation.

(4) The competition network will be comprised of twelve virtual machines configured to perform network functions at a small company. Blue Teams will have a discovery period during which they will learn the details of each of the systems with which they will be working (e.g. server or workstation, critical services, etc.).

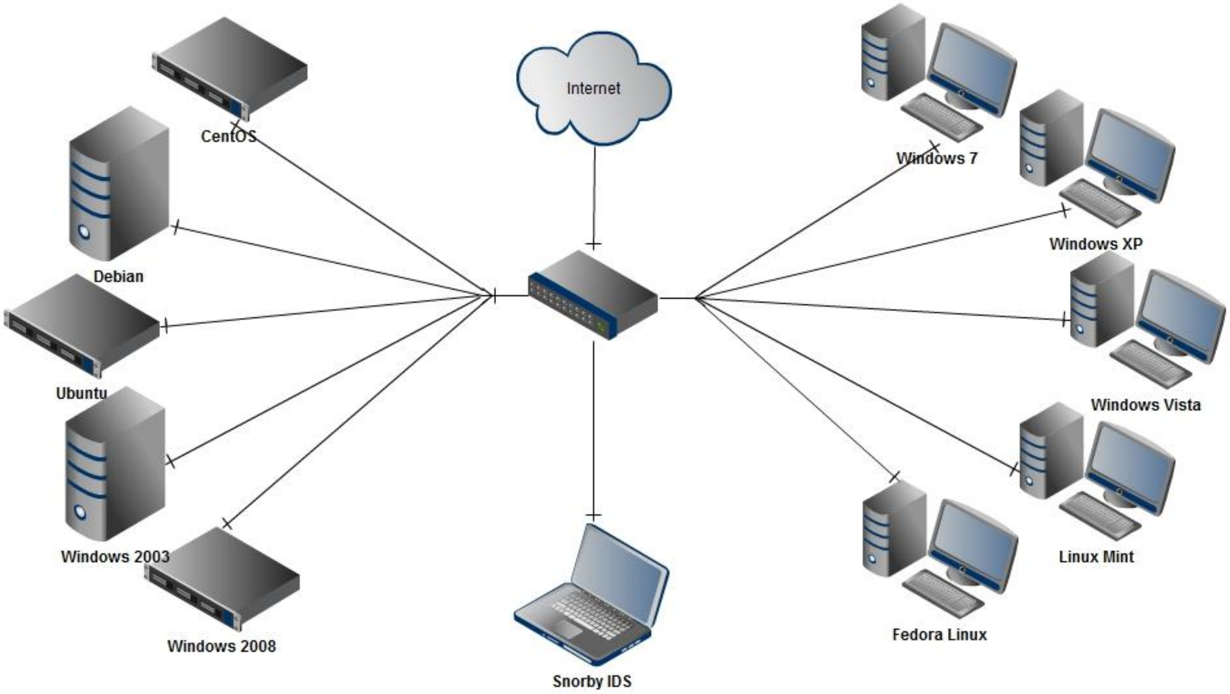
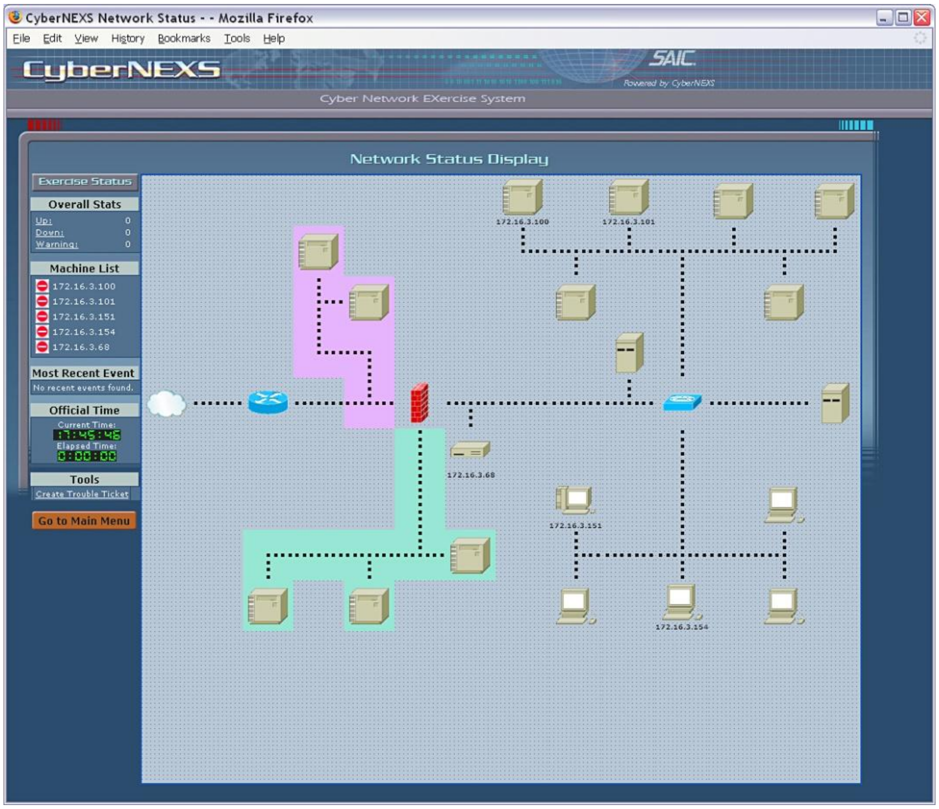


Figure C-1 – CyberNEXS Network



Overall Stats

Up: 0
Down: 0
Warning: 0

Machine List

- 172.16.3.100
- 172.16.3.101
- 172.16.3.151
- 172.16.3.154
- 172.16.3.68

Most Recent Event

No recent events found.

Official Time

Current Time: 17:45:46

Elapsed Time: 0:00:00

Figure C-2 – Blue Team System Status Board

4. Competition System Failover and Restart Procedures

a. General. Though the competition staff will do their best to ensure system outages do not occur, we must be prepared for a system outage and continue our competition operations.

b. Competitor Note Taking. It is ***critical*** that the competitors **take notes** of their actions throughout the competition, so that they may reset their systems to the same levels of security as before an outage.

c. Outage during 1st Half (Pre-2.5 Hours). In the event of a system outage lasting more than 20 minutes, the Commissioner, CyberPatriot Program may decide to initiate a system failover process. The decision to initiate the system failover process will depend on the time left in the competition, normally before the 2.5 hour mark of the competition. The process should take 40 minutes or less. Once the failover process is initiated and completed, competitors will restart the competition with clean images and no score.

d. Outage during 2nd Half (Post-2.5 Hours). In the event of an outage that occurs after the 2.5 hour mark of the competition that lasts for one hour or longer, the Commissioner, CyberPatriot Program may decide to terminate the competition. At that point, the most recent scores may count as the teams' final scores.

e. Competition Network Outage /Failover Timeline

(1) Failover Conditions

(a) Competition session is less than 2.5 hours old
(b) 20+ minute sustained outage

(2) Actions

(a) Students take notes on SysAdmin and other actions
(b) Local CyberNEXS node is activated (40 min)
(c) Teams reset (15 minutes) actions before Red Team penetrations
(d) Competition Continues

(3) Outage during 2nd Half (Post-2.5 Hours)

(a) Teams wait one hour for restoral.
(b) No restoral after one hour -- teams depart competition floor

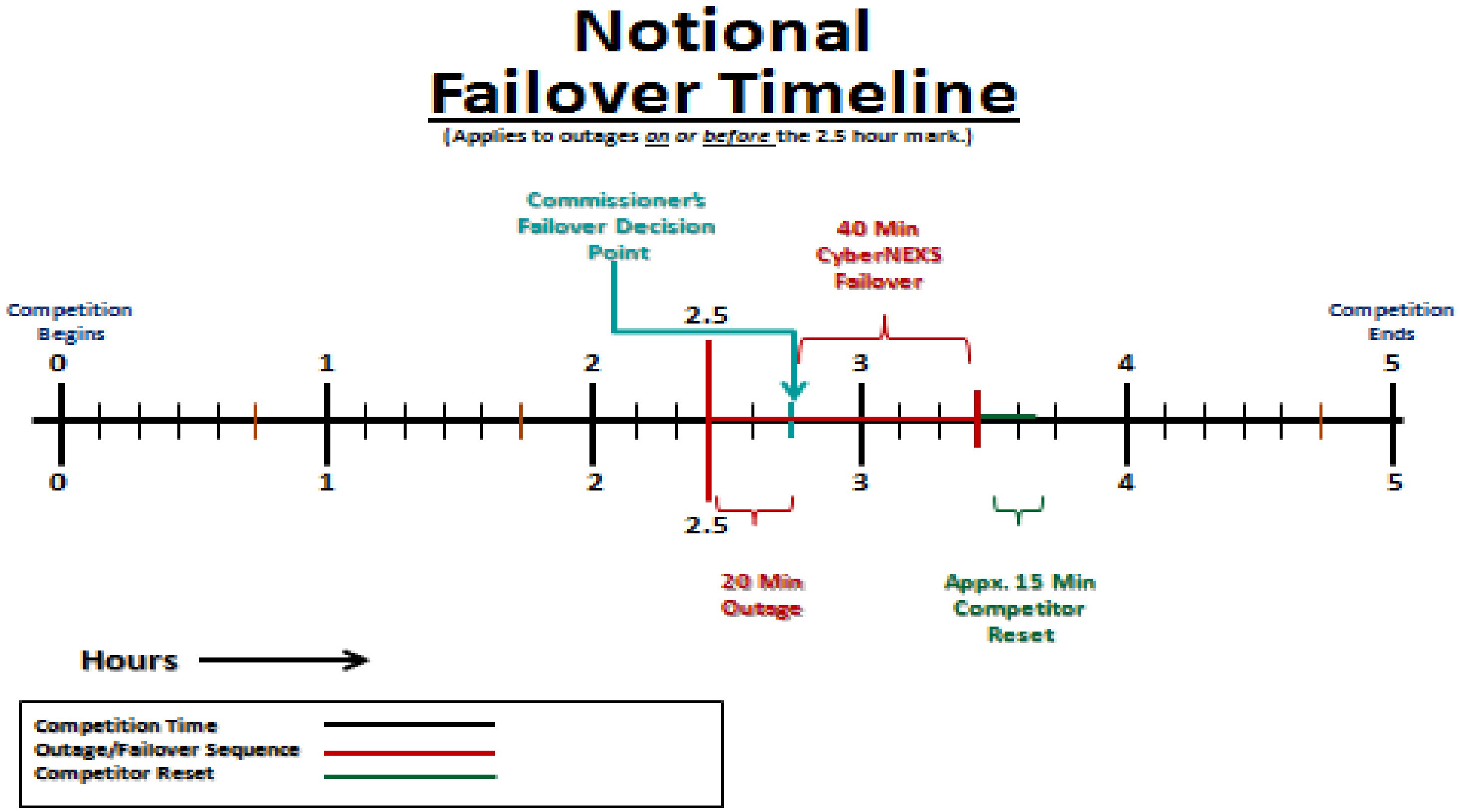


Figure C-3 – Notional Failover Timeline

g. <u>Scoring Actions</u>

(1) Local CyberNEXS scores may be used for the Network Security Competition scores, if a failover is executed and the competition restarted. The previous scores may not be considered if the failover is successful. It is ***<u>critical</u>*** that the competitors **<u>take notes</u>** of their actions throughout the competition, so that they may reset their systems to the same levels of security as before the outage.

(2) For an outage that occurs after the 2.5 hour mark, the last CyberNEXS scores may be used for final Network Security Competition scores.

SECTION D. Forensics Competition

Table of Contents

Paragraph

Attachments

POC: Frank Zaborowski
F.zaborowski@uscyberpatriot.org, 703-247-5840

1. Forensics Competition Overview

The Forensics Competition will be conducted by the Department of Defense Cyber Crime Center (DC3) using the DC3 Crime Scene Challenge.

All information necessary to successfully compete (and win!) will be provided to teams as part of team orientation. No prior knowledge or training is necessary.

The object of the DC3 Crime Scene Challenge is for participants to use forensic and investigative skills to focus on potential digital evidence and conduct triage/analysis of such evidence. Teams are given a scenario and an interrogation script of a suspect. The scenario and script outline that there is vital information to be found – without it, the suspect must be let go! It is the team's job to review the case information and analyze the scene quickly.

Participants need to find all the evidence items and the key device with the vital information stored on it in less than 15 minutes. Points are awarded for each evidence item found and secured, for identifying the key device, and finding the vital information on the device. If there is a tie with points, the team with the fastest time will be first. We hope this challenge educates participants on the issues Investigators currently face, while keeping their attention through a fun and interactive competition.

2. Preparation

a. In this guide is a scenario in which a cyber crime has been committed. Along with the scenario will be an interrogation script from a previous interrogation of the suspect. Participants are asked to read the scenario and interrogation scripts, analyze the situation, and develop leads. Teams are allowed to read these as many times as they wish and take them into the scene with them, if they so choose.

b. Teams are required to read the rules of the challenge before they enter the scene. If the teams have any questions before they enter the scene, they may ask a DC3 staff member at the 'Registration' desk. Once teams enter to compete, they are assumed to have read the rules and fully understand proper and improper behavior as well as possible consequences.

c. Team Roles. We advise that teams with more than two members divide up into "roles." Members can take on more than one "role." Both members on two-member teams will assume all roles. Teams with three and four members do not need to have a "Lead Investigator." Typical personnel involved in cyber Investigations include, but are not limited to:

(1) Digital Forensic Examiner: An individual who is responsible for imaging, analyzing, and reporting on digital evidence provided by an investigator. (During this competition, the Digital Forensic Examiner will not be imaging or reporting, only analyzing evidence on-site. This practice is called "Triaging" evidence.)

(2) Evidence Custodian: When the Evidence Custodian is called on-site, he or she is typically in charge of telling the investigators how to seize certain items, where the items need to go, and

records the items on a "Chain of Custody." (During this competition, the Evidence Custodian would stand next to the table marked for digital and non-digital items and determine which items should be placed on which side.)

(3) Lead Investigator: An individual who is responsible for a case. This person would delegate responsibilities to other agents and determine which items are pertinent to the case and should be seized. (During this competition, the Lead Investigator would not search the scene, but manage team members. Team captains would fit this position, but are not required to do so.)

(4) Responding Agent(s): The first person on scene who is responsible for securing the area, ensuring evidence is not tampered with or destroyed, and collecting the evidence. (During this competition, the Responding Agent(s) will be actively searching and seizing items from the scene. They will also be handing over evidence to the Evidence Custodian. We recommend only two team members for this role.)

3. Forensics Competition Description

a. Once the team arrives to compete, members will be given latex gloves to put on and then led into the crime scene as a team. (IMPORTANT: If anyone is allergic to latex, please let us know for an alternative solution.)

b. When all team members are inside the scene, it will be their responsibility to identify and secure all evidence items and analyze only one seized device for digital evidence within a 15-minute time frame.

c. In the crime scene, there will be two tables. One table will have a black, Dell laptop. The other table will be divided into two sections – one section marked "DIGITAL DEVICES", and the other marked "NON DIGITAL DEVICES". These tables are NOT part of the crime scene and do not need to be searched. They are part of the investigative work area where you will store, secure, and analyze evidence.

d. To secure a digital device, place it on the table side marked "DIGITAL DEVICES" and describe the item to the DC3 team for scoring.

e. Other items, considered non-digital, should be placed on the table side marked "NON DIGITAL DEVICE" and describe the item to the DC3 team for scoring.

f. The one digital device the participants choose to analyze must be correctly attached to the forensic laptop after being approved by the DC3 team.

g. Choose the correct evidence device on the first try to gain 15 more points.

h. If an incorrect device is chosen, the DC3 staff member will state "Improper device" and the participant will have to search for another. Five points will be deducted each time this occurs.

i. Once the team is approved by DC3 staff member for analyzing the digital device on the "forensic laptop," they may attach it and retrieve the vital information from the device.

j. When the correct evidence from the digital device is found, show it to the DC3 staff member and tell them the search is complete to stop the time and submit the score.

k. Once time is up, the score is submitted and participants must leave the area without touching anything. Teams can see their ranking for the Crime Scene Challenge on the television screen by the DC3 registration booth.

NOTES:

- This competition is worth 10% of teams' final scores for the CyberPatriot National Finals Competition.
- Some evidence items are harder to find and are worth more than others. The winners of this challenge are the teams with the most points, so be sure to try and find all the evidence items before searching for digital evidence. In the event of a tie with points, time will be used as the tie-breaker.

4. Crime Scene Challenge Rules

a. **Do not** remove any items from the scene. Inventory is taken after each team completes the investigation.

b. **Do not** behave or act inappropriately with the suspect; show respect for them.

c. The only non-evidence items to be taken off the suspect are ones that would be required to come off at an airport security check-point.

d. **Do not** plug in a device to the forensic machine that the DC3 Staff has not approved.

e. **Do not** touch DC3 Staff members or photographers in an inappropriate manner.

f. **Do not** break any items in the crime scene.

g. **Do not** bring cell phones or other recording devices into the scene.

h. **Do not** discuss any details of the crime scene with friends; it is a competition.

i. **Do not** enter the scene without a DC3 staff member or other crime scene administrator.

j. **Do not** take down signs or logos without prior consent from a crime scene administrator.

k. **Do not** use the equipment in any way for malicious purposes.

l. **Do not** cheat.

m. **<u>Do have FUN!</u>**

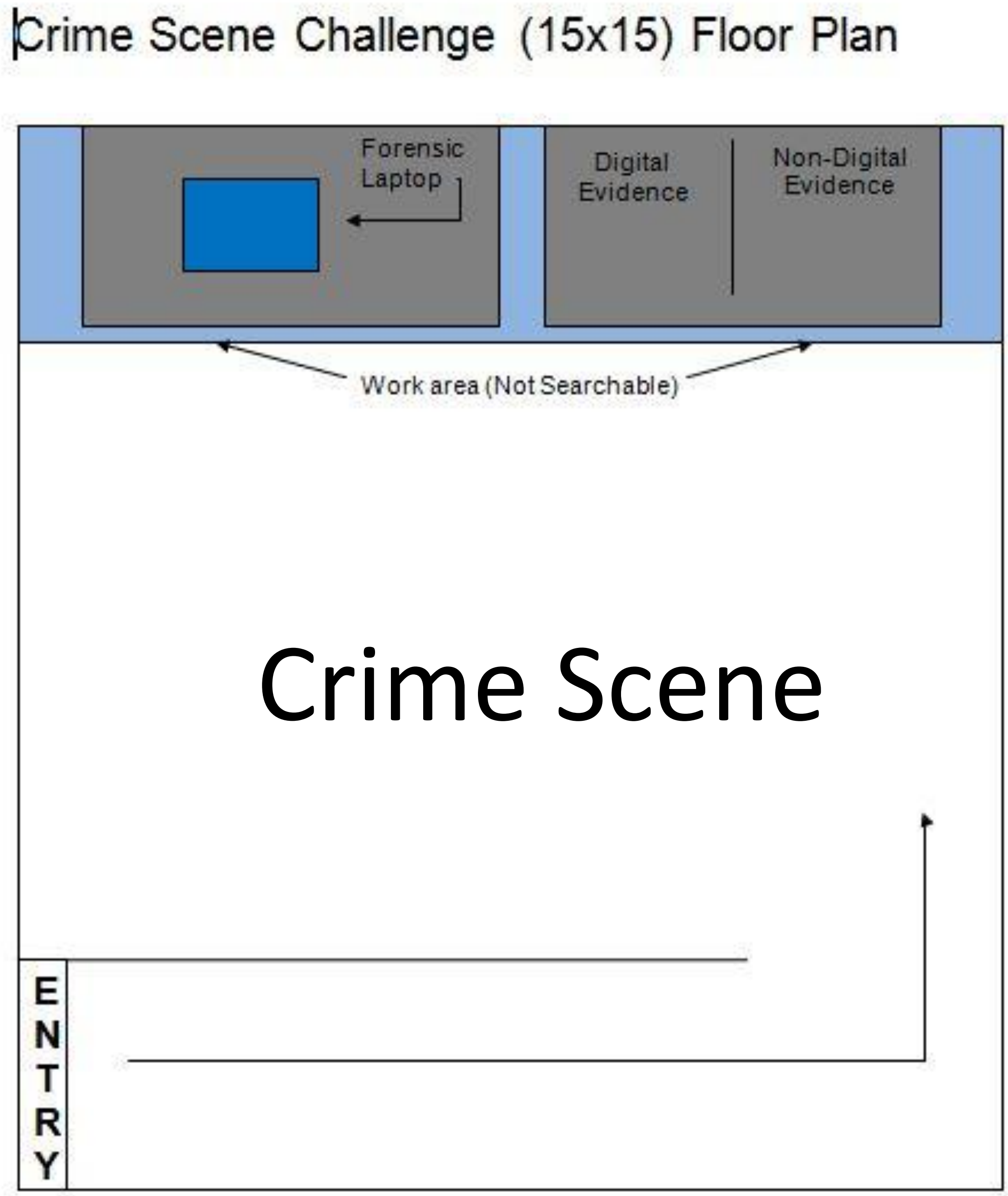


Figure D-1

Crime Scene Scenario

- **You are the Chief Security Officer for a large corporation.**
- **The security guard of the corporation informed you that they believe an employee is stealing company information.**
- **The guard noticed on video surveillance tapes that the employee entered restricted areas, to which they do not have authority to enter.**
- **The CEO gave permission to search the employee's desk.**
- **A search was discreetly conducted at his desk last night.**
- **Electronic devices were found that did not belong to the company and are not permitted in the building.**
- **Also found were letters from a business competitor addressed directly to the suspect.**
- **Upon exiting the building today, the employee was detained and questioned by the security guard.**
- **After the questioning, you were called in to search for hidden devices and analyze any digital evidence.**

Attachment 1

<u>Interrogation of Suspect - Script</u>

Q- Mr. Jermer, have you been entering a restricted area of this facility?

A- No

Q- Sir, we have you on tape. Let me ask you again, have you been entering the Research and Development area, to which you do not have permission to enter?

A- ….yes

Q- Why have you been visiting that area?

A- To talk to colleagues.

Q- The area is clearly marked as restricted and each employee is briefed when they are first hired here that the area is off limits to all but the R&D team. Why couldn't you wait to talk to your colleagues?

A- Because I needed some information, and they told me they would let me in.

Q- How did you get in?

A- Maggie O'Connor gave me her access card

Q- Why would Ms. O'Connor give you her own access card? Wouldn't she need it for work?

A- She was on vacation. She gave it to me so I could use it while she was gone.

Q- So you lied before when you said that you went in to talk to colleagues?

A- No! I needed to get some information from her and she said she'd let me in. She gave me her card.

Q- That sounds like lying to me. You got information from her, but there was no talking involved. Before, you said you entered to talk to colleagues. That's the second time you've lied to me.

A- Whatever

Q- Was anyone else aware that Ms. O'Connor gave you her access card?

A- No.

Q- What information were you looking for?

A- Our kids are on the same soccer team. My wife wanted to invite the other parents and their kids to a get together at my house. She had the team roster saved to her computer. She gave me her card, I went in, got the roster and left.

Q- Why would she have a kid's soccer roster on her work computer in a restricted area? And why couldn't you get it from someone else?

A- She's the coach of the team. She probably just e-mailed it to herself and then saved it to her desktop.

Q- So then Ms. O'Connor had the roster at her house to be able to send it to herself at work. Why couldn't you just get the one she had at home?

A- I don't know, like I said before, she PROBABLY e-mailed it to herself. I don't know how SHE put it on there. I just know that was where she told me to look after I asked for it.

Attachment 2

Q- The company does not allow storage devices/media in the building that doesn't belong to the company. Why did you have personal electronic devices at your desk?

A- Everybody sneaks in their phones, iPods, CDs, and things like that. The work here is so monotonous that we all need something to entertain us otherwise we'd go crazy.

Q- The video surveillance shows you entering R&D twice. Why twice?

A- I left my pen. I had to go back and get it.

Q- What is so special about your pen?

A- It's my favorite. I always keep it with me. Plus, I didn't want anyone else to take it.

Attachment 2