SANS Institute Submission 2 to the Cybersecurity Workforce RFI

How to Rapidly Accelerate the Growth of a Highly-Skilled U.S. Cybersecurity Workforce (Based on Findings from the United Kingdom's and UAE's Multi-Year Pilot Programs)

> *Response to question 8: "What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the nation's cybersecurity workforce?"*

Summary: This RFI response provides a recommendation that will enable the United States to accelerate the development of a large, highly-skilled cybersecurity workforce. It includes findings that led to the United Kingdom's, June 2016, $25 million launch of its CyberSchools program providing a starter template for the U.S. initiative. The United States CyberStart program will, in 36 months, motivate more than 100,000 American high school and college students to have fun and learn while, at the same time, assessing their interest and talent in cybersecurity. For those with talent and interest, CyberStart will enable them to develop their skills. An extension of the program will enable the U.S. military services to find undiscovered cyber talent among enlisted personnel and officers so that their cyber skills can also be developed, as well.

Contact Information: Alan Paller, Director of Research, The SANS Institute, apaller@sans.org

Recommendation: Launch a United States CyberStart program, within 180 days, to enable 100,000 American high school and college students to be motivated to learn about cybersecurity and find out whether they have the natural talent and perseverance to excel in the field. For those who have talent, CyberStart will develop and validate their foundational skills required for excellence in technical cybersecurity roles.

Because of the intense hands-on skills CyberStart participants will master, they will be prepared to immediately start being productive in the workforce. This program, which can be completed in 36 months, is a scaled-up U.S. adaptation of a program that has been run effectively (with measurable, remarkable results) in the UAE and that was launched nationwide in the United Kingdom this summer.

Findings on Which CyberStart's Effectiveness Rests

Pilot tests of early versions of CyberStart identified three barriers that can be eliminated and when eliminated enable rapid growth of skilled cybersecurity people:

> Barrier 1: The "wall" that students hit when a technical cybersecurity topic (buffer overflows) is introduced and they have not yet mastered the underlying technology (basic programming). The "wall" forces teachers to change their classes from deep-technical, hands-on courses to survey courses leaving the students without usable skills.
>
> Barrier 2: The differences in both previous skills development and psychometric measures among students. These differences when not addressed lead to capable but less experienced students being left behind and feeling inadequate and may lead to their giving up.
>
> Barrier 3: The boredom students feel when they are lectured to or given large numbers of exercises without a narrative tying them together. It's tough to pay attention when you are bored. It's tough to learn when you are not paying attention.

CyberStart

CyberStart has three elements that have proven capable of overcoming those barriers:

(1) CyberStart Assess: A simple test combining psychometric and skills assessment that reliably separates students into those who are likely to excel, those who need a boost but can succeed and those for whom technical cybersecurity is just too hard.

(2) CyberStart the Game: A highly motivating game of discovery and challenge that can be played anywhere there is an internet connection, and that has more than 300 hours (400 by December 2017) of challenges. It finds and develops interest and hands-on skills in the foundations and basics of cybersecurity.

(3) CyberStart Essentials An intensive hands-on, online and live training program providing deep mastery of the foundations of cybersecurity as well as common attacks.

What students say about the CyberStart game (these are the first U.S. users: Montgomery College students who used CyberStart to qualify for a new cybersecurity course (names and contacts available)):

> *"It gave us hands on experience with many types of the techniques that we learned about in our coursework. I find that learning by doing is much more memorable and enables me to more thoroughly understand what I am learning as opposed to just reading about it in a textbook or watching an instructionalvideo."*
>
> *"We were given the freedom to approach the challenges in whatever way we wanted. If we got stuck, we could skip that particular challenge and move on. I also liked the fact that Cyber Protection Agent Field Manual was included and that we could consult it at any time. It really helped me better understand how I should approach the given challenges. Lastly, I liked the narratives. It's a detail that I feel helped with continuity, as opposed to just laying out a bunch of challenges with no story to get you invested in their outcome."*
>
> *"It allowed me to test myself on real problems in this field. The challenges were structure in the right way - easy to understand what they wanted and how they wanted."*
>
> *"The coolest part was that it was all available online and that it had some hidden meaning and interesting ways to guide you through the challenges while teaching you relevant security methods and techniques."*
>
> *"I really liked the way it enabled me to use new and different techniques to solve the challenges. It forced me to read and browse and learn in order to solve the challenges."*

CyberStart testing in the United States:

- NSA/NSF GenCyber Camps in New Jersey, Alabama and Illinois are using CyberStart as a mentored activity, under an NSF grant that includes assessment by an independent evaluator. (The Galante report that justified use of CyberStart in GenCyber camps is attached.)

- The governors of Virginia, Nevada, Delaware, Hawaii, Rhode Island and Iowa offered CyberStart to high school and college students during a three week period in July, 2017. In the first 17 days, 3,000 students are playing the game, testing their interest and talent in 8 CyberStart challenges. More than 1,300 of those students completed sufficient numbers of those 8 CyberStart challenges to win access to the full game, with hundreds of increasingly sophisticated and educational challenges, for the month of August. Evidence is mounting that even the 8-challenge evaluation program motivates interest in cyber. Here's what a talented computer science student at Iowa State wrote On August 1st.

> *"Even if I don't get invited to the main CyberStart Game this has really piqued my interested in cyber security. I really enjoyed these challenges!"*

He is being invited to the main game. The nation needs tens of thousands more talented young people to get their "interest piqued."

==end==

Implementation of the Cyber Protection Agent Game in GenCyber Camps

An analysis by Mandy Galant: award winning high school teacher (winner of both the NJ AFA Teacher of the Year award and the Yale Educator award), coach of the 4th place nationall Cyber Patriot Team in 2015 and leader of New Jersey GenCyber Camps.

CTFs are a great cyber learning tool but they can be exclusionary - Capture the Flag (CTF) competitions are a valuable learning tool - nothing motivates like a contest and a prize! But there can be a steep learning ramp to playing CTFs and often they are crafted so that prior knowledge is necessary for success. It can become a negative experience where new players feel like everyone else “knows stuff” and they feel shut out. The result is that many players hit a wall, can’t make any progress and then give up on CTFs. Students can’t learn if they feel shut out and aren’t playing the game!

CPA provides a friendly intro to CTFs that overcomes the barriers to entry - Using the Cyber Protection Agency (CPA) game, we can level out the learning ramp to CTFs. The early stage CPA challenges introduce players to foundational concepts so they can accumulate enough of the “stuff” everybody else already knows. At every point in CPA there is scaffolding for new concepts through the Field Manual, Hints and search tips. This means that a player always has easily accessible resources and won’t face any game-ending points of frustration. If we want to expand the community of students who are learning from challenging CTFs, it makes sense to reduce the exclusionary nature by giving everyone the keys to the club.

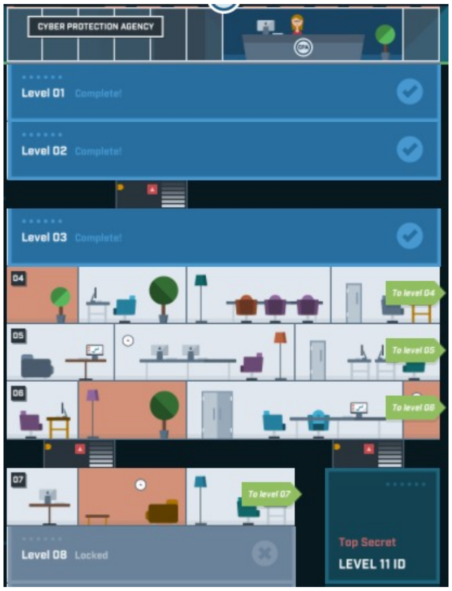
CPA fits into the mission of GenCyber - The Cyber Protection Agency game can be a valuable tool towards achieving the goals of the GenCyber program which are to “develop cybersecurity awareness and teach sound cybersecurity fundamentals at the K-12 levels and improve teaching methods for delivering cybersecurity content in K-12 computer science curricula.” CPA can be implemented in GenCyber camps as an instructional practice exercise, as a daily scheduled activity or as a full CTF competition.

Cyber Protection Agency (CPA) Game Overview

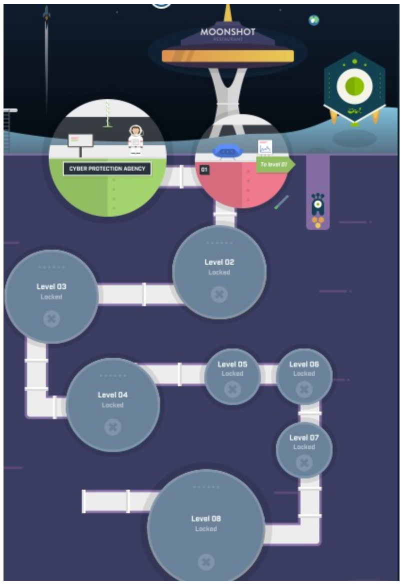
Age Level - middle school (grades 6-8) through high school (grades 9-12).

1. **Bases** - Headquarters and Moon - these are the portals to levels.
   Note that with two Bases there are effectively TWO complete CTF games

Headquarters

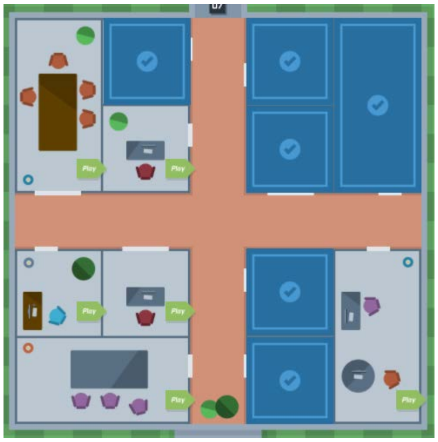


Moon Base

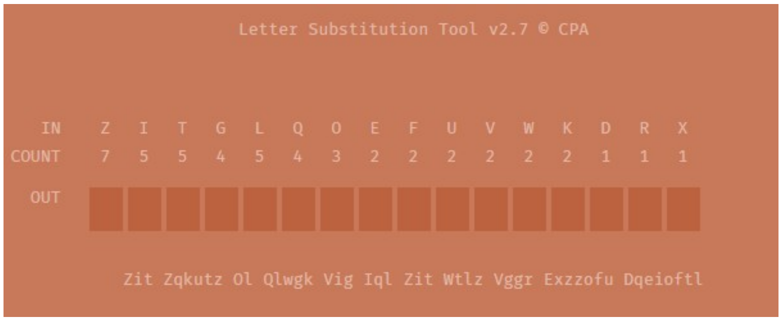


2. **Levels** - each level has 12 challenges and the next level is unlocked after a certain number are completed. Players don't need to complete the entire level to move to the next - as something makes sense later, the player can come back to apply that new knowledge. Learning doesn't have to be linear; it is problem-based and unique to each person's challenge preference.

Level with 12 Challenge rooms



Example Cryptography Challenge



```
             Letter Substitution Tool v2.7 © CPA

   IN   Z  I  T  G  L  Q  O  E  F  U  V  W  K  D  R  X
COUNT   7  5  5  4  5  4  3  2  2  2  2  2  2  1  1  1

  OUT   □  □  □  □  □  □  □  □  □  □  □  □  □  □  □  □

      Zit Zqkutz Ol Qlwgk Vig Iql Zit Wtlz Vggr Exzzofu Dqeioftl
```

3. **Challenges** are distributed across multiple categories including:
   - Online Safety & Social Engineering
   - Cryptography
   - Encoding
   - Basic Linux Command Line
   - Python programming

- Web Security & Javascript
- File Forensics
- Programming Overflow Errors
- URL Manipulation
- SQL Database manipulation

Note: CPA does not follow a "Jeopardy" style format as the challenges do not have labeling to indicate category. The player will first use deduction to determine the proper approach to a solution.

4. **Help resources**:
   - The CPA Field Manual provides basic instruction on each of the category concepts. Some players will opt to learn first, and then play - others will use it as a resource as they go through the game.
   - Optional hints are available for each challenge but the player must forfeit points to access them. This provides an incentive for players to try to solve challenges without help, but ensures that players will not hit a wall and will continue to positively experience the game.
   - A narrative briefing sets up the scenario for each challenge. The information in the briefing provides the player with a basis to start searching online for solution methods. This helps students to improve their Google searching skills, a key talent needed to succeed at CTFs and in life!

Using Cyber Protection Agency Game in GenCyber camps

Scenario 1 - instruction with CPA game as practice exercises

GenCyber teachers select a Category as an instructional topic and incorporate specific CPA challenges as practice activities to reinforce learning concepts. CPA comes with an Instructor Resource Guide that includes:

a. category identification of challenges by level and room.
   Example: Level 1, room 12 = Python
b. the flag and short "how-to" for each challenge
c. difficulty of each level - i.e. level 1 & 2 are easiest, level 3 slightly more challenging, etc.

Using the guide, teachers can assign specific challenges that are topic related. Because the campers have received instruction on that category, the challenges will be very accessible and competency will be achieved quickly. Since the teachers have an answer guide, they can provide additional "soft" hints in cases where campers struggle too long with a challenge.

Example:

Instructional topic = What is the difference between Encoding and Encryption?
Difficulty level = Easy to Low-Medium
Challenges to complete = Level 1 (1, 4, 7, 8, 12) and Level 2 (3, 4, 7, 9, 11) and Level 3(6, 7, 11, 12)

Scenario 2 - scheduled daily activity for length of camp

The GenCyber Camp uses the CPA game as a team or individual daily activity that is not directly tied to any specific instruction or lesson. Students can select whichever challenge they want and move through the game at their own pace.

To enhance student engagement, camps can use the CPA provided game posters. Hang the CPA game posters on the classroom walls, one for each team of campers. Each team has an assigned color and as they complete a challenge they put one of their colored stickers in that challenge room.   This provides a visual connection to team accomplishments and an ongoing, low-key “scoreboard” for the camp CPA game.

Scenario 3 - full CTF competition

The GenCyber Camp would schedule the CPA game as a true CTF competition including a common start and stop time for all campers. The game can be held during part or all of a camp day or can be played 24/7 over several days if all students have access to computers and Internet at home.

Winners would be based on the CPA game points and prizes can be awarded based on highest score, age level or fastest time to reach a game level. Competitions are a fun way to end the camp with high-energy.

Scenario 4 - teacher camps

GenCyber camps that are focused on teacher training will use the CPA game as the foundation for creating curriculum materials. The GenCyber trainers will introduce the basics of the concept. Teachers will work their way through a challenge or group of category related challenges. After learning and CPA game practice, teachers will then create a How-To or full lesson plan to bring back to their classroom.

Alternatively, the CPA game can be integrated into the teachers camp as a way to expose teachers to the CTF concept and inspire them to recruit their students into CTF competitions during the school year.

==end==