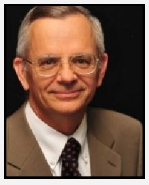
ISSUE 46 | JAN 2016

The CyberSentinel

The official newsletter of CyberPatriot—AFA's National Youth Cyber Education Program

Commissioner's Cache



Happy New Year! I hope you had a wonderful holiday.

2015 ended with exciting results from Round 2. It was great to see so many teams do so well. And 2016 promises to be an even more exciting year! January will bring an exciting State Round in which ALL high school teams may participate, no matter past round participation. And the Regional Round in February will lead to another energetic National Finals Competition at a new location, the Baltimore Inner Harbor, in April.

Our Elementary School Cyber Education Initiative will be significantly updated this year, and the number of AFA CyberCamps will be expanded.

We could not do any of this without the support of our Presenting Sponsor, the Northrop Grumman Foundation, and our other generous sponsors listed on page 4. We appreciate all they have done and continue to do for CyberPatriot and the future of our nation.

Good luck with the State Round, and a Happy CyberPatriot New Year!

Bernard K. Skoch | National Commissioner

DATES TO KNOW

JAN 4.	AFA Re-opens
JAN. 29-31	State Rounds (HS)
JAN. 29-31	Practice Round 2 (MS)
FEB. 19-21	Regional/Category Rounds (HS)
FEB. 19-21	Semifinal Round (MS)

2016 AFA CYBER-CAMPS COMING SOON!

The CyberPatriot team is gearing up for its second season of AFA CyberCamps - are you ready?!

This exciting summer camp program includes curriculum and software kits designed to introduce novice students to cyber ethics, online safety, and fundamental Windows and Ubuntu security tools.

Registration will open mid-March: stay tuned for more information as registration approaches.

Round 2 Ends — All High School teams on to State Round

With a hard-fought ending to Round 2, the Qualification Rounds came to an end at 10:00 p.m. ET ,on Dec. 6. When the round started on Dec. 4, no one could have predicted the course it would take. With the large number of perfect scores in Round 1, the round could have easily been a repeat for many teams. The addition of the Cisco Networking Challenge quiz and an additional image showed the mettle of the competitors.

Image scores were respectable considering the much increased difficulty over the Round 1 images. Cisco Networking Challenge quiz scores were high. After Round 2, the Rounds 1 and 2 scores were combined. High school teams were assigned to Platinum, Gold, and Silver Tiers based on their scores The top 50% of middle school teams made the Semifinals.

Next up is the State Round, Jan. 29-31. ALL high school teams may compete no matter their placement in Rounds 1 and 2 or even if they did not compete in one or both rounds. Based on the teams' performance in Rounds 1 and 2, teams are assigned to tiers for the remainder of the season. Each of the tiers will compete with a set of challenges specifically for their performance level.

The Middle School Division will have a Semifinals Practice Round during the State Round. The round will provide an opportunity for the teams to practice before the Semifinals scheduled for Feb. 19-21.

A list of CP-VIII images and Cisco Networking Challenges for the remainder of the rounds can be found at: www.uscyberpatriot.org under the Latest News announcements or **HERE.**

Air Force Association | 1501 Lee Highway | Arlington, VA 22209
info@uscyberpatriot.org | 877-885-5716 | www.uscyberpatriot.org

Publisher: B. Skoch | **Editor:** R. Dalton
Asst. Editor: F. Zaborowski

JAN
16

Cyberthreats to Watch for in 2016

It's no secret that cyberthreats are a serious issue. As we successfully address security measures for existing threats, new threats continue to appear. Cybersecurity is a world of ever-changing peril, and the only way to mitigate the risk on a personal level is to be aware of both where and how you could be effected. Take a look at some of the biggest cyberthreats to watch out for in 2016:

Cloud Computing: Cloud computing is an easy way to store vast amounts of data without taking up any physical space. Out of mind, out of sight… but not for hackers.

Mobile Devices: Mobile devices are a great way to have information at your fingertips, but they are also a target for hackers. Forty-three percent of "bring your own device" smartphones used by US workers don't have a password, a personal identification number or pattern lock. Fifty percent use these devices to connect to unsecured Wi-Fi at least once a month, and nearly half of mobile apps on any given mobile device have at least one major security flaw.

Infrastructure: Most people think of personal information being stolen during a security breach, but they don't think of how many other aspects of everyday life are controlled by computers. Many security experts worry about the possibility of US infrastructure (utilities, telecommunications and logistics) becoming the next major target of cybercriminals.

Automobile Hacks: Automobiles are as structurally sound and safe as ever, but from a technological standpoint, they are more vulnerable. As more and more cars connect to the Internet for such functions as GPS, they become more vulnerable.

EMV Chip Cards: During 2015, US credit card companies began issuing EMV (Europay, MasterCard and Visa) compliant cards, that use an integrated circuit instead of a magnetic strip for data storage. While this change is intended to reduce certain types of fraud, it will also give cybercriminals a new avenue of attack—card-not-present (CNP) technology.

Phishing Attacks: Phishing is certainly not a new cyberthreat, but experts believe it will continue to be prevalent. As long as people keep falling for phishing scams, phishers will keep on phishing.

CryptoWall: CryptoWall is a form of ransomware that makes computers unusable until victims pay the criminal who infected their computer with it. Backing up computers on a daily basis is an easy way to avoid the heartache of a CryptoWall attack.

Medical Devices: The newest threat for medical devices will be 'ransomware/Stuxnet' attacks, where hackers can tap into the administrative privilege capabilities of medical devices, which are typically restricted to manufacturers or hospital administrators.

Source: ***http://www.cnbc.com/***

How many programmers does it take to change a light bulb?

None. It's a hardware problem.

Sponsor Profile: NCG

The University of Maryland announced in November a renewed commitment of $2.76 million from the Northrop Grumman Foundation to its Advanced Cybersecurity Experience for Students (ACES) program.

The ACES program – the nation's first honors program in cybersecurity – was launched by UMD's Honors College in 2012 with support from the Northrop Grumman Foundation to address a critical, national strategic need. Since its inception, the ACES program has offered 65 percent more credits than originally targeted and served 50 percent more students than originally anticipated. ACES began as a living-learning program for freshman and sophomore students. With this renewed commitment, the program will now expand to offer a more advanced cybersecurity curriculum to juniors and seniors, culminating in an ACES minor.

"The support that the Northrop Grumman Foundation has committed in support of the ACES program shows how important this type of workforce is to the nation," says Mary Ann Rankin, UMD's senior vice president and provost. "This generous gift will allow us to continue to educate and train our students to be future cybersecurity leaders and meet the growing needs in the nation and state."

"We are delighted with the growth of the ACES program and the surge of interest among students from several dozen different disciplines at the University of Maryland," says Sandra Evers-Manly, President, Northrop Grumman Foundation. "We hope that our continued support will help the program reach and attract an even greater and more diverse population of students." (continued on page 4)

The gift from the Northrop Grumman Foundation will allow

Coaches' Corner

- **Online Coaches and Mentors Meetings.** The Coaches Meetings are a great time to ask any questions about the upcoming round of CP-VIII! The format will be an interactive chat session. Information on joining these meetings will be emailed to Coaches a few days before the meeting. Additional questions can be directed to info@uscyberpatriot.org.

  Next Meeting: Jan. 19, 9:00 a.m.—5:00 p.m.

- **Participant Kits.** Due to the significant amount of program growth this season, we are currently waiting for additional inventory to be delivered. While a large majority of the kits have already been packed and shipped, some orders have incurred inventory-related delays. We apologize for the wait and appreciate your patience! The remaining kits will be sent in early/mid January. Mentor and team assistant kits will be sent separately, directly to the individual's address of record.

SPOTLIGHT: COMAL INDEPENDENT SCHOOL DISTRICT

CYBERPATRIOT PROGRAM TEACHING VALUABLE LESSONS CRITICAL TO OUR NATION'S FUTURE

Written by Jason Gordon, Communications Coordinator, Comal ISD

Dec. 1, 2015— Cyber-based crime is at an all time high and as a result it's a problem our youngest generation will have to deal with for the rest of their lives.

Comal ISD's leadership is certainly taking an active role in giving its students a chance to learn about the national CyberPatriot program.

CyberPatriot was conceived by the Air Force Association (AFA) to inspire high school students toward careers in cyber-security or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.

"I think it's very important for our students to be actively involved in programs like CyberPatriot," said Andrew Kim, Comal ISD superintendent. "There is a skilled-trained workforce shortage in cyber security. By talking to and involving students as young as the elementary level we can definitely grow a pipeline of young men and women interested in cybersecurity education."

Comal ISD currently has 28 total teams of four students apiece throughout the district at the middle and high school level. These teams not only participate in events such as CyberPatriot clinics held at San Antonio College and Rackspace, but will also take part in a virtual competition against schools from other districts throughout the year.

Comal ISD's high school and middle school CyberPatriot teams will also visit the district's elementary schools to teach students about cyber security, online security and digital citizenship.

"I'm very excited CyberPatriot is part of Comal ISD's long-term vision," said Keven Harshbarger, Smithson Valley High teacher and CyberPatriot coach. "It's a tremendous opportunity for our students who are interested in learning about Information Technology (IT) and cyber security. Currently, there are 500,000 unfilled cyber security jobs. Even if our students don't pursue this career path, being in the CyberPatriot program teaches them new ways to explore and problem solve."

Participation in the CyberPatriot program has required support from the district's technology department, campus principals and teachers, and Comal ISD administration. For example, Mike Turner and Brenda Sendejo, of Comal ISD's technology department, jumped at the chance to mentor both students and coaches.

"You could really see the excitement in one particular student's eyes I was talking to," said Turner. "He was so interested in how everything in this program worked. I think that's the overall theme with the CyberPatriot program, everyone loves the fact they are learning advanced computer skills while having fun at the same time."

Comal ISD also relies on mentors in the community who possess IT skills, such as Randy Muennink, of Gruene Technology Group. Muennink said it's difficult to find qualified applicants in the IT field.

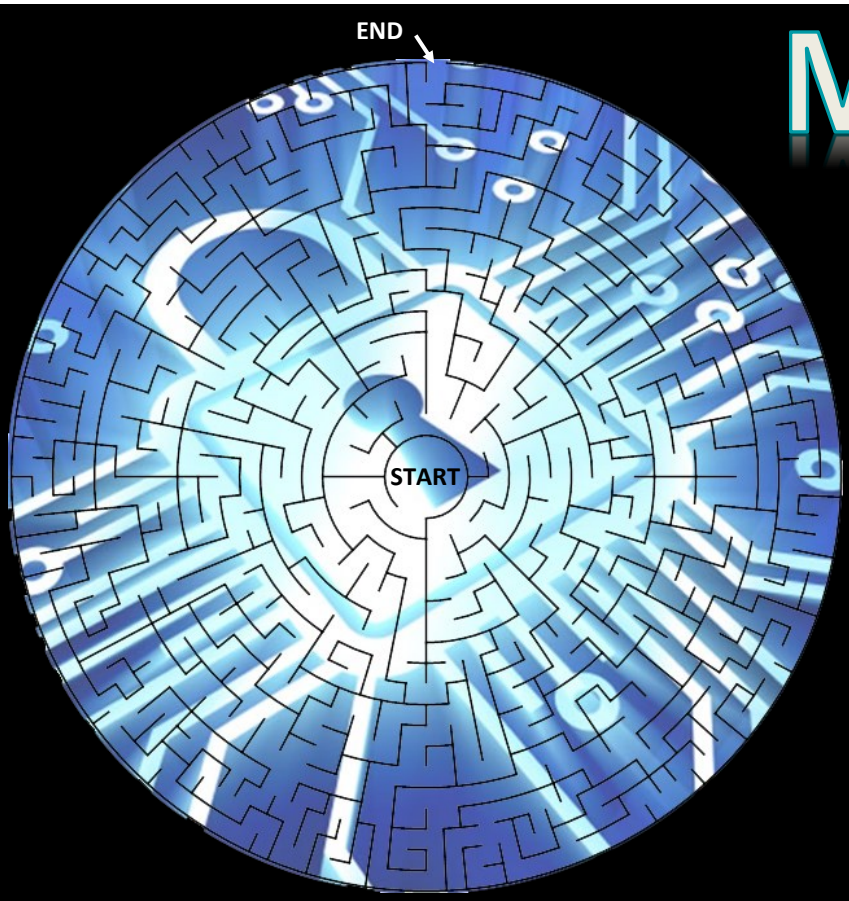
"It's great Comal ISD gets behind something like this," Muennink said. "This field is something that's not always addressed. I'm constantly looking to hire people and I can't find them. As far as being a mentor goes, we were looking for ways to give back, and this seemed like a perfect fit. We believe strongly in education and we know IT security is a growing need for all employers."

Sami Theurer, teacher and CyberPatriot coach at Church Hill Middle, agreed the program has had a direct impact on her students.

"Technology changes on an hourly basis for the generation we're teaching now," said Theurer. "This program really opens a new window of knowledge for our students. It provides many different ways to use that technology positively."

IN PHOTO: Church Hill Middle seventh-grade student Riley Muennink receives a Comal ISD CyberPatriot program backpack from superintendent Andrew Kim. Kim delivered backpacks, which include a lanyard with a flash drive attached, a journal and pens, to each of the coaches and students district-wide involved in the program.

JAN
16



MAZE.EXE

Can you escape the maze?

Time yourself and let us know if you're faster than the fastest CyberPatriot staff member?

FASTEST TIME (Leslie):

36 seconds

NCG (CONTINUED)

ACES to prepare a larger, more diverse student body for leadership roles in this burgeoning field through extended instruction and program administration; an enhanced experiential learning environment; scholarships for recruiting and retaining a diverse, high-achieving student body; and dedicated spaces on campus for the ACES program to thrive.

Northrop Grumman and the Northrop Grumman Foundation are committed to supporting cybersecurity education, training and technology. In addition to CyberPatriot and the ACES program, the foundation supports the University of Maryland Baltimore County (UMBC) Cyber Scholars program; the company also leads the Cybersecurity Research Consortium and is partnered with bwtech@UMBC on the Cync incubator program.

This Month In Cyber History

Jan. 19, 1983 — On this day in cyber history, Apple introduced the Lisa Computer. Development for the Lisa Computer began in 1978. It was to feature a graphical user interface (GUI) and use the Motorola 68000 CPU. It was also the first Apple product with an internal hard drive.

Steve Jobs, head of the project until he was taken off it in 1982, initially claimed LISA stood for Local Integrated System Architecture, though later admitted it was named for his daughter, Lisa Nicole Brennan. The Lisa sold for ten thousand dollars, which along with poor third party software availability and incompatibility with the Apple II, led to weak sales. In 1985, the Lisa was rebranded the Macintosh XL at less than half the cost of the original Lisa. Despite increased sales, the Mac XL was discontinued later in 1986, bringing an end to the Lisa story.

For more information, visit:
http://www.computerhistory.org/tdih/January/19/