AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT ONE

Introduction to CyberPatriot and Cybersecurity

www.uscyberpatriot.org

SECTION ONE

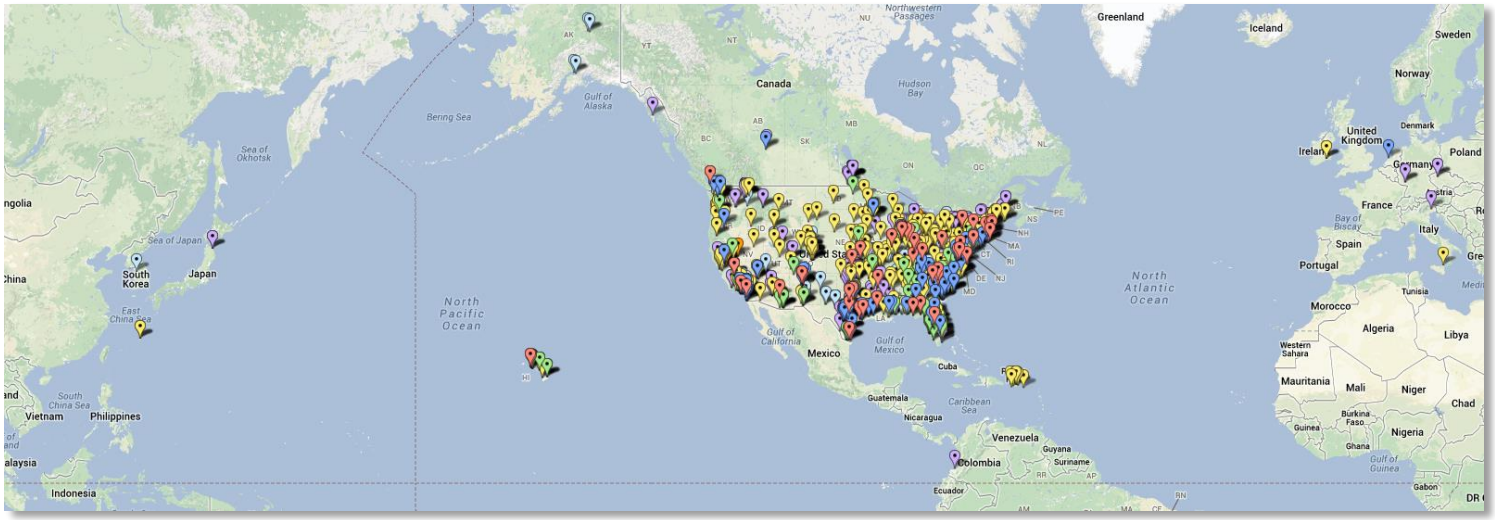
Introduction to CyberPatriot

What Is CyberPatriot?

- The National Youth Cyber Education Program
  - AFA CyberCamps
  - Elementary School Initiative
  - National Youth Cyber Defense Competition
- **Not** hacker training
  - Offensive behavior is not tolerated
- Fun way to learn skills that will be useful in the future
  - Technical skills
  - Teamwork
  - Critical thinking

The National Youth Cyber Defense Competition

- Teams consist of 2 to 6 Competitors, a Coach, an optional Technical Mentor, and an optional Team Assistant
- Teams compete in online qualifying rounds
- Points are earned by identifying and correcting weaknesses in a simulated computer system



The National Finals Competition

- Top teams earn all-expenses-paid trips to Washington D.C.
- More than just competing in front of a computer: Digital Crime Scene Challenge, Cisco Networking Challenge, and other additional components
- Opportunity to win scholarships, network with industry leaders, and enjoy media recognition

What is CyberPatriot?

Click here to play the CyberPatriot recruitment video:
http://www.youtube.com/watch?v=Q_TbXri0XQ0

How CyberPatriot Works: Team Structure

- Coaches act as administrative lead of the team
  - Supervise students
  - Act as main point of contact for CyberPatriot Program Office
  - Ensure integrity of the competition
  - If technically savvy, train teams for competition
- Technical Mentors volunteer to help Coaches train teams
  - Use industry expertise to teach students about cybersecurity
  - Guest lecture or work with team(s) on a regular basis
- Team Assistants volunteer to provide non-technical support and encouragement to the team
- Competitors work together to find and fix vulnerabilities in a simulated computer system

Click here for more information:
http://www.uscyberpatriot.org/competition/how-it-works/team-organization

How CyberPatriot Works: Scoring

- Earn points by fixing vulnerabilities in a virtual machine (VM)*
  - Virtual machines (aka “images”) are software programs that simulate computer systems
- Lose points for making the system less secure
- Harden your system and defend against outside attacks by starting with hints and the scenario in the ReadMe file on the desktop
- Not all vulnerabilities are scored or hinted at in the ReadMe
  - You might do something that improves the system, but does not earn your team points
  - The goal of the competition is to harden the system as completely as possible in the provided time

*More information on VMs is available in Unit Three of these training materials

How CyberPatriot Works: CCS

- The CyberPatriot Competition System (CCS) automatically transmits your team's progress in the competition image (VM) to the CyberPatriot scoring server
- Use the CyberPatriot Scoring Report to check your score and your connection status and score
- A chime will play when you gain points and a buzzer will sound when you lose points
- Do not open, modify, or delete anything in the "CyberPatriot" folder of any image
  - Doing so could cause you to lose your progress in the image

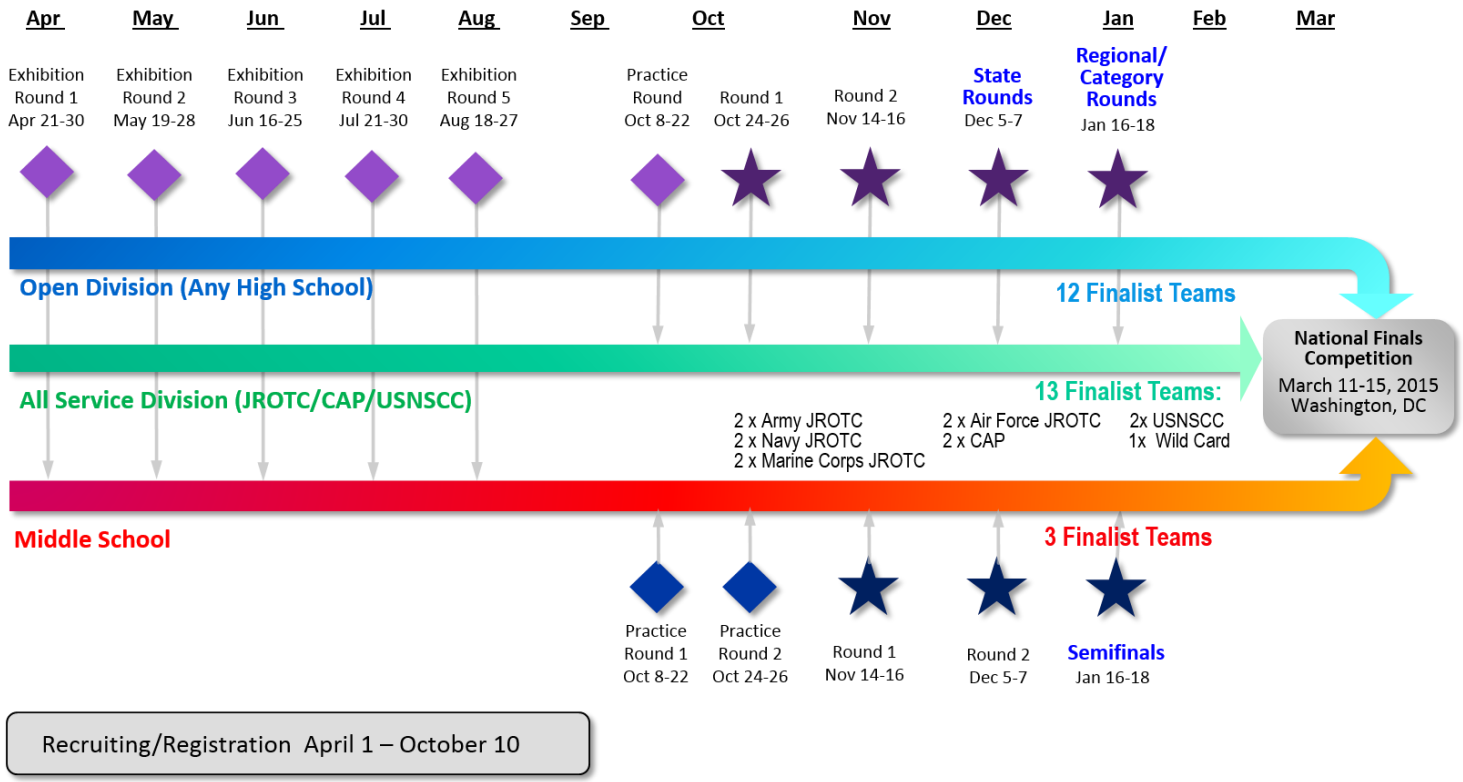
How CyberPatriot Works: Competition Deployment

SAMPLE SCHEDULE:

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2	3	4 Competition Round Preparation Email sent	5
6	7	8	9	10	11	12
13	14 Image Download and Instructions Email sent	15	16	17	18 StartEx Email sent COMPETITION	19
20 ROUND	21	22	23	24	25 Round Results Email sent	26
27	28	29	30	1	2	3

- Competition emails are only sent to registered Coaches
- Preparation Email contains information on types of images in the round and competition updates
- Image Download and Instructions email includes download links and thorough instructions for the round
- StartEx contains password to unzip images and log into user account
- Teams choose a six-consecutive-hour window during the competition weekend to compete. Six-hours must fall between support times posted by CPOC.

CyberPatriot VII Timeline



Click here for more information:
http://www.uscyberpatriot.org/competition/competition-timeline

Important Resources

- The CyberPatriot VII Rules Book
  - Click here: http://www.uscyberpatriot.org/competition/rules-book
- Training Modules available on your team's Coach's Dashboard
- Additional Windows resources
  - Click here: http://www.uscyberpatriot.org/competition/training-materials/windows
- Additional Linux resources
  - Click here: http://www.uscyberpatriot.org/competition/training-materials/linux
- Additional Cisco resources
  - Click here: http://www.uscyberpatriot.org/competition/training-materials/cisco
- Ubuntu practice images and Windows scoring engine provided by Texas A&M Corpus Christi
  - Click here: http://www.uscyberpatriot.org/competition/training-materials/practice-images

SECTION TWO

Introduction to Cybersecurity

What is Cybersecurity?

All the tools we use and actions we take to keep computers, networks, and information safe and available for those who need it, and unavailable for those who should not have it.

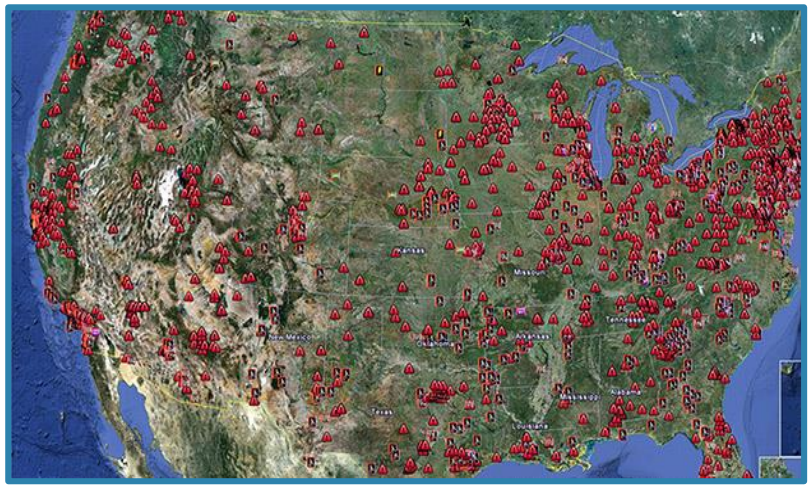
That means protecting hardware and data from everything from hacktivists to earthquakes

Source: www.UMUC.edu

Why is Cybersecurity Important?

Things that rely on computers:

- Banks
- Factories
- Schools
- Airlines and Railroads
- Stores
- Police and fire departments
- Military and government systems
- Doctors' offices



Source: US Department of Homeland Security

⇨7,200+ critical American industrial control systems are linked to the Internet, and therefore vulnerable to attack

Answer: Cybersecurity isn't just about protecting computers.
Almost everything relies on or could be affected by a computer.

Why is Cybersecurity Important?

- **2006:** 26.5 million veterans' personal information is compromised after the theft of a Veteran Affairs employee's laptop. The employee thought it was safe to bring home VA records on an unsecure drive.

- **2009:** Coca-Cola executive clicks link in spoof email allowing attackers to steal confidential files on $2.4 billion business deal with Chinese juice company.

- **2011:** DHS plants USB drives and CDs outside of government and government contractor buildings. The majority are picked up by employees and inserted directly into their organization's computers.

Answer: People make mistakes.

Cybersecurity is often about protecting organizations and individuals from themselves.

Sources: CSO magazine, www.csoonline.com, Bloomberg News, www.bloomberg.com, GCN Magazine, www.gcn.com

Why is Cybersecurity Important?

Case: RSA Security Services

Source: blogs.rsa.com

- RSA: security firm that sells SecurID®
- Lockheed Martin: a $46 billion defense contractor that uses SecurID®

Attackers infiltrate RSA's network through malware deployed in spoof emails sent to the company's employees

Criminals capture the algorithms used to generate Lockheed Martin's random SecurID® passwords

Criminals launch attack on Lockheed's networks using the algorithms they stole from RSA

Luckily, Lockheed's security team is able to thwart the attacks.

Answer: We're all connected

A weakness in one system can be exploited by attackers to target another system.

Source: InformationWeek, http://www.informationweek.com/security/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013

Who's Hiring?

- Nearly every organization needs cybersecurity professionals
- 300,000+ new information technology jobs were created in 2013
- Average salary for computer jobs in 2013 was ~$89,000, while cybersecurity-specific jobs brought an average salary of $100,000+

Source: Computer World, http://www.computerworld.com/s/article/9237394/Demand_for_IT_security_experts_outstrips_supply?pageNumber=2

Cyber Career Opportunities

- Cyber workers
  - Employees that maintain day-to-day security and strengthen their organization's protection
- Cyber defenders
  - Government or contractor employees that protect American networks and information from attacks
- Cyber sleuths
  - Professionals that watch for espionage and insider threats and perform digital forensics for law enforcement
- Cyber leaders
  - Industry veterans that decide company security policies, train new employees, and conduct R&D