PRESIDENT'S CUP
CYBERSECURITY COMPETITION

President's Cup Cyber Competition

Finding the Best Cyber Talent in the Federal Government

EXECUTIVE ORDER 13870 – AMERICA'S CYBER WORKFORCE EO

- (e) The Secretary of Homeland Security, in consultation with the Secretary of Defense, the Director of the Office of Science and Technology Policy, the Director of OMB, and the heads of other appropriate agencies, shall develop a plan for an annual cybersecurity competition (President's Cup Cybersecurity Competition) for Federal civilian and military employees. The goal of the competition shall be to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines. The plan shall be submitted to the President within 90 days of the date of this order. The first competition shall be held no later than December 31, 2019, and annually thereafter.

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- Executive Order 13870 – The competition plan shall address the following:
  - (i) The challenges and benefits of inviting advisers, participants, or observers from non-Federal entities to observe or take part in the competition and recommendations for including them in future competitions, as appropriate;
  - (iii) The parameters for the competition, including the development of multiple individual and team events that test cybersecurity skills related to the NICE Framework and other relevant skills, as appropriate. These parameters should include competition categories involving individual and team events, software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, cyber-physical systems, and other disciplines;

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- Executive Order 13870 – The competition plan shall shall address the following:
  - (iv) How to encourage agencies to select their best cybersecurity practitioners as individual and team participants. Such practitioners should include Federal employees and uniformed services personnel from Federal civilian agencies, as well as Department of Defense active duty military personnel, civilians, and those serving in a drilling reserve capacity in the Armed Forces Reserves or National Guard;

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

Requirements

- Had to be accessible from anywhere
- Minimum Hardware/Software requirements for end users
- First round open to all .gov/mil

Qualifiers

- Jeopardy format
- First round open to all
  - Over 1,000 participants
- Second round downselect
  - Top 20% of teams
  - Top 100 individuals
- Final Round
  - Top five teams
  - Top ten individuals

Teams Round 1 Gameboard

ANALYZE AND INVESTIGATE	COLLECT AND OPERATE	OPERATE AND MAINTAIN	PROTECT AND DEFEND	SECURELY PROVISION
250	250	250	250	250
500	500	500	500	500
1000	1000	1000	1000	1000

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

Open-Source Resources

- TopoMojo
  - Quick deployments of small virtual environments for hosted challenges
- Gameboard
  - Application to manage scoring and run a competition on top of TopoMojo
- Allowed for unique challenge types
  - Example - “Build the Road”

Challenge Development

- Make as many downloadable as possible
- Variants
  - Multiple of each variant for each challenge deployed at random
  - “Infinity challenges” – procedurally generated variants
- Participation Timer to Level Playing Field
  - Competition open for ten days, participation limited to eight hours
  - Influenced challenge development, influenced competitor strategy
- Challenge QA is Key to Successful Competitions

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

Cyber Escape Room

- 3D immersive environment coupled with cyber challenges
  - Extensive testing to ensure “video game element” did not detract from ability to solve the cyber challenges
  - All IT/OT in game engine faithfully replicated in virtual network environment
  - Clicking on a terminal brings up the appropriate VM
  - Can move USB drives between workstations to transfer tools and files
- How to encourage teamwork?
  - Challenges frequently required two competitors to work together, one in 3D environment and one in VM

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

LIVESTREAM

- Incorporate non-Federal participation
- Highlight excellence among competitors
- Training value
- Additional content
  - Interviews, speeches, challenge solves
- https://youtu.be/jxXYDSJnhwM

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

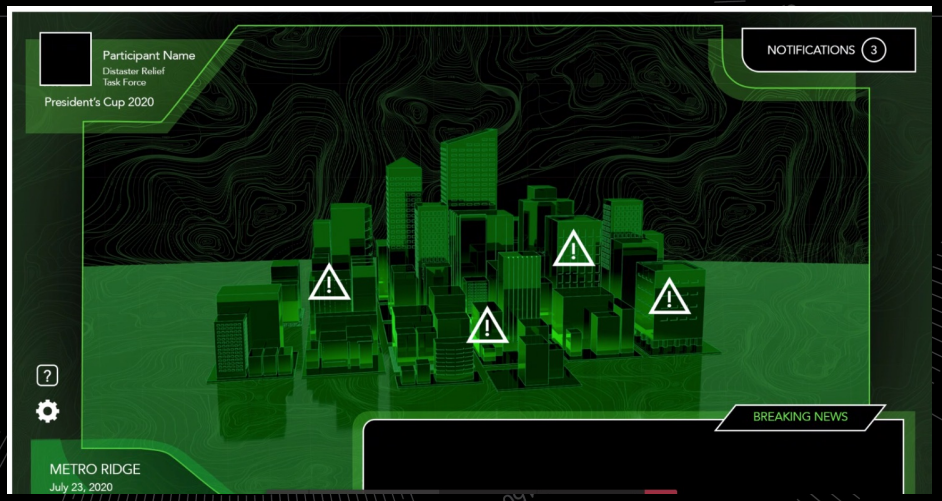
Year Two Improvements

- Implementation of partial-credit challenges with multiple parts to fully solve
- Individual Tracks
  - 4 hour competition instead of initial 8 hours
  - Split into two separate competition tracks along focus areas:
    - Track A – Incident Response, Forensics
    - Track B – Vulnerability Analysis, Exploitation Analysis

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

Adapting the Escape Room for a Remote Competition

- Required GPU to run escape room application
- How to keep minimal hardware/software requirements, as available as possible?
- Cloud GPU-enabled Virtual Machines to access the game client



PRESIDENT'S CUP
CYBERSECURITY COMPETITION

CISA

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

”Save the World” Challenges

Enduring Value of Competitions and President's Cup

- Competitions offer a unique way to provide training, education
- Competitions are a valuable way to gauge cybersecurity hands-on skills
- Competitions offer opportunities for beginners to engage with cybersecurity challenges
- Hosted Challenges Available for Feds – presidentscup.cisa.gov
- Hosted Challenges Available for BlackHat Attendees – bh.presidentscup.cisa.gov
- Platform, challenges are open-source (github.com/cmu-sei) (github.com/cisagov)
- Virtual Appliance to be released in August
  - Can be used to build your own challenges, competitions, training

PRESIDENT'S CUP

CYBERSECURITY COMPETITION

FOR MORE INFORMATION: **CISA.GOV**

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — CISA