PRESIDENT'S CUP
CYBERSECURITY COMPETITION

President's Cup Cybersecurity Competition

Building a Competition Across the Federal Workforce

What is the President's Cup Cybersecurity Competition?

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

- America's Cybersecurity Workforce E.O. 13870 mandates DHS to hold the competition annually.

- The goal of the competition is to identify and reward the top cybersecurity talent in the federal workforce.

- Any federal executive department or agency employee can participate, including uniformed service members.

- Participants can compete as an Individual, on a Team of up to five members, or both.

2021 Winners		
Individual Track A USMC	**Individual Track B** USAF	**Team** 780th Military Intelligence Brigade

President's Cup Format

- The competition has three rounds – two Qualifying Rounds and Finals.

- Qualifying Rounds
  - Must succeed in first qualifying round to participate in second round
    - Teams – best team from each Department, plus top 20% based on score
    - Individuals – Top 100

- Final Round
  - Top 5 Teams and Top 10 Individuals in Tracks A/B
  - Day 2 of Teams Finals Livestreamed via YouTube

Considerations for President's Cup Platform

- Accessible anywhere from a standard web browser
    - Minimum Hardware/Software requirements for end users

- Scalable to support potentially thousands of concurrent participants across the federal .gov/.mil

- Open-Source Resources
    - TopoMojo – https://github.com/cmu-sei/TopoMojo
    - Gameboard - https://github.com/cmu-sei/Gameboard
    - Identity - https://github.com/cmu-sei/Identity

President's Cup Challenge Development

- Each challenge is tied to a NICE Work Role

- Built within TopoMojo
  - Multiple variants of each challenge created and deployed at random
  - "Infinity challenges" – variants within challenge randomized by TopoMojo

- Quality Assurance for each challenge
  - Playtesting conducted by National Labs with support of DOE

- Session timer
  - Influences challenge development and competitor strategy

Where's the site?

There was an update to a mission critical website, but we don't know where the new site is. Can you help?

NICE Work Roles:

Exploitation Analyst

NICE Tasks:

- T0266 - Perform analysis for target infrastructure exploitation activities.

President's Cup 2019 Wrap-Up

- **Two Tracks – Teams and Individuals**

- **Two Qualifying Rounds per Track**
  - **"Game-show" style**
  - **Held remotely over 10 days with 8-hour time limit**

- **Final round consisted of 3D immersive "Escape Room"**

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

00:27:03

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

President's Cup 2020 Wrap-Up

- **Multi-part challenges with partial credit**

- **Individual Tracks**
  - **Track A – Incident Response, Forensics**
  - **Track B – Vulnerability Analysis, Exploitation Analysis**

- **Remote Finals**
  - **Cloud hosted "Save the World" Game**
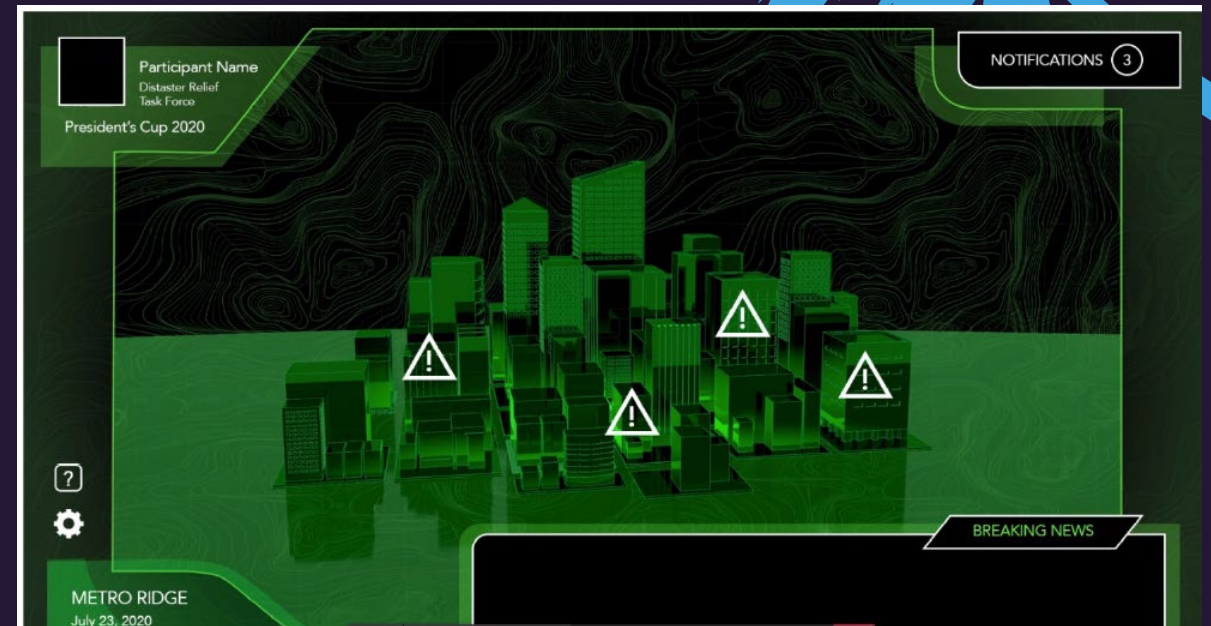
President's Cup 2021 Wrap-Up

- Continue using NICE work roles for Teams and Individuals Tracks

- Updated Gameboard

- Remote Finals
  - Save the planet narrative

Gameboard Updates in 2021

- **Consolidated Gameboards into a single application**

- **Integrated challenge metadata**

- **Migrated email functionality away from Gameboard**
  - **PII protections**

Outlook for President's Cup

- Expand use of President's Cup challenges
  - Hold additional internal competitions for federal workforce.
  - Make existing challenges available to provide training opportunities through simulated real-world environments.

- Releasing source code of challenges to public after each competition.

- Foundry Appliance – Announced at 2021 Blackhat

PCCC Practice Area
Practice demo challenges and content from past President's Cup competitions

- 2021 Practice
  Gameboard
- Challenge Archive
  Gameboard
- Open Source Challenges
  GitHub
- Walkthrough Videos
  YouTube

Foundry Appliance

- Pre-configured VM that packages President's Cup applications

- Single-host Kubernetes cluster to replicate production deployment

- Uses VMware ESXi to serve virtual challenge environments

- https://github.com/cmu-sei/foundry-appliance

Carnegie Mellon University
Software Engineering Institute

Foundry Appliance v0.4.0

Welcome to the Foundry Appliance. This virtual machine hosts workforce development apps from the Software Engineering Institute at Carnegie Mellon University.

Getting Started

The appliance advertises the *foundry.local* domain via mDNS. All apps are served as directories under this domain.

To get started using the virtual appliance:

1. Download root-ca.crt and trust it in your keychain/certificate store. This removes browser certificate warnings.
2. Navigate to any of the apps in the following two sections.
3. Unless otherwise noted, the default credentials are:
   ```
   user: administrator@foundry.local
   pass: foundry
   code: 123456
   ```

Foundry Apps

The following Foundry applications are loaded on this appliance:

PRESIDENT'S CUP
CYBERSECURITY COMPETITION

PRESIDENT'S CUP

CYBERSECURITY COMPETITION