# CAE Tech Talk

## 16 December 2021

**President's Cup Cybersecurity Competition: Building a Competition Across the Federal Workforce** (1:00 – 1:50 pm EST)

**AI for Cybersecurity and Cyber Security for AI** (2:00 – 2:50 pm EST)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. CAE Tech Talks are free and conducted live in real-time over the Internet so no travel is required. Capitol Technology University (CTU) hosts the presentations using Zoom which employs slides, VOIP, and chat for live interaction. Just log in as "Guest" and enjoy the presentation(s).

Below is a description of the presentations and logistics of attendance:

### PRESENTATION #1

**Topic:** President's Cup Cybersecurity Competition: Building a Competition Across the Federal Workforce

**Time:** 1:00pm – 1:50 pm EST

**Location:** https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

**Presenter(s)**: Michael Harpin, Cybersecurity and Infrastructure Security Agency, Cyber Defense Education and Training (CDET)

**Description:** In 2019, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) held the first cybersecurity competition for the Federal workforce. The goal of the President's Cup Cybersecurity Competition is "to identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines". To be able to reach the entire federal workforce in the .gov/.mil, CISA and the Software Engineering Institute (SEI) built a platform accessible to all interested participants with minimum end user requirements. Now in the third year of the

President's Cup, CISA is looking to improve the experience of the participants while also making the competition's material available to the public.

## PRESENTATION #2

**Topic:** AI for Cybersecurity and Cyber Security for AI

**Time:** 2:00pm – 2:50 pm EST

**Location:** https://captechu.zoom.us/j/664120328

Just log in as "Guest" and enter your name. No password required.

**Presenter(s)**: Dr. Anupam Joshi, University of Maryland, Baltimore County

**Description:** Two technologies are growing in importance -- AI and Cybersecurity. Not only are they individually important, their intersection is also growing in importance. Large datasets are now available to detect attacks. These come from not just the traditional sensors like those on networks and hosts, but also from textual sources such as web fora, dark web, and threat intelligence feeds. AI can help us make sense of these large volumes of data to support SoC analysts in their tasks. However, as we deploy AI systems, they also present a new attack surfaces for adversaries to exploit. Attacks range from poisoning the models being learned, fooling them with adversarial examples, and inferring the data that was used to train the model. In this talk, we will explore both these elements. While we will also introduce our research, the primary purpose is to make the audience aware of the challenges and developments in this space.

**CAE Tech Talks are recorded; view them here:** https://www.caecommunity.org/resources/cae-tech-talk-resources

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov