NICE FRAMEWORK SUCCESS STORY
President's Cup Cybersecurity Competition
Cybersecurity and Infrastructure Security Agency

Talent Management

The voluntary [Workforce Framework for Cybersecurity](#) (NICE Framework) was developed through a collaborative process by industry, academia, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

ORGANIZATIONAL PROFILE

The [Cybersecurity and Infrastructure Security Agency](#) (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. CISA's programs and services are driven by a comprehensive understanding of the risk environment and the corresponding needs identified by public and private stakeholders.

As part of Executive Order 13870: America's Cybersecurity Workforce, CISA founded [the President's Cup Cybersecurity Competition](#) in 2019 as a national cybersecurity event aiming to identify, challenge, and reward the best cybersecurity talent in the Federal workforce. The competition was made available to any Federal executive department or agency employee, including uniformed service members.

The competition consists of two qualifying and one final round, each increasingly more difficult. The challenges generally use a capture the flag format, but the final teams round is an immersive simulated environment. Real-world scenarios are used for the challenges where participants will apply technical skills to solve a problem or complete a task.

DRIVERS

E.O. 13870 called for the President's Cup Cybersecurity Competition to be held on an annual basis. Per the executive order, "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 Executive Order also required the President's Cup competition activities be mapped to the NICE Framework and other categories (software reverse engineering and exploitation, network operations, forensics, big data analysis, cyber analysis, cyber defense, cyber exploitation, secure programming, obfuscated coding, cyber-physical systems).
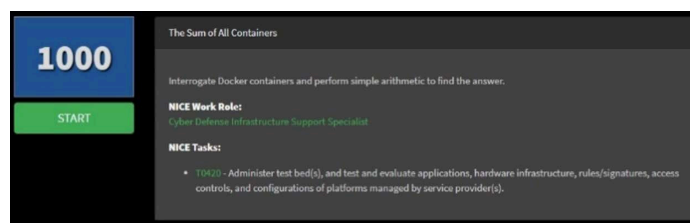

Figure 1: Screenshot of President's Cup gameboard

PROCESS

For each President's Cup Cybersecurity Competition, CISA requires that each challenge be mapped to the NICE Framework. This ensures that the competition is well-rounded and covers a wide variety of knowledge and skills.

For the inaugural competition in 2019, challenges focused on the categories listed in the Executive Order and categories from the NICE Framework. Of the seven NICE Framework Categories, Oversee and Govern was not included in the competition, while Analyze and Investigate were combined into one category to make five distinct categories. All competitors were tested across the NICE Framework in keeping with the Executive Order.

In 2020, the individual competition was divided into two specialized tracks. One for Incident Response and Forensics and the other for Exploitation and Vulnerability Assessment. This allowed participants to compete in areas that most closely align to their skillset, although individuals could choose to participate in one or both tracks based on their interest.

Challenges in the 2020 competition were mapped to Work Roles and Tasks within the NICE Framework, rather than Categories. The Work Roles and Tasks for each individual and team competition were selected based on the President's Cup staff's experiences and insights from developing the challenges.

In the competition's gameboard, the NICE Framework Work Roles and Tasks were identified for each challenge to make it easier for participants to decide which challenges to attempt. Direct links to relevant NICE Framework Work Roles and Tasks were also included in the challenge instructions.

TIE-IN WITH THE NICE FRAMEWORK

Mapping the competition challenges to the NICE Framework helps the President's Cup meet its goal to challenge participants across a variety of cybersecurity disciplines.

> "The President's Cup Cybersecurity Competition identifies the top cybersecurity talent in the Federal workforce and is tied to the NICE Framework. By using the Framework, the competition ensures that the finalists demonstrate the wide breadth of knowledge and skills required to address the evolving cyber threats of today and tomorrow."
>
> -Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA

In the future, CISA plans to collaborate with agencies and departments to identify what Work Roles are in-demand or heavily staffed across the Federal government to identify areas in which the challenges will best align.

BENEFITS & IMPACT

Aligning the competition to the NICE Framework has worked well to develop challenges that not only test a variety of skills but also are grounded in real-world scenarios.

Shifting the focus from the NICE Framework Categories to the Work Roles and Tasks added value to the competition. It kept the competition from being too heavily focused on certain cybersecurity skillsets.

CISA has published the 2019 President's Cup challenges and plans to do the same with the 2020 challenges. The NICE Framework information is detailed for each challenge to assist individuals to seek specific challenges for education and training.

CISA will continue to use the NICE Framework Work Roles when designing future President's Cup Cybersecurity Competition Challenges.

CONTACT INFORMATION & RESOURCES

Contacts:
▸ Michael Harpin, Federal Lead, President's Cup Michael.harpin@cisa.dhs.gov
▸ Education@cisa.dhs.gov

Websites:
▸ www.cisa.gov/presidentscup
▸ presidentscup.cisa.gov/
▸ github.com/cisagov/prescup19-challenges

April 2021