CYBERSECURITY SKILLS JOURNAL: *PRACTICE AND RESEARCH*

Call for Proposals
Special Issue: NICE Framework
2023 Volume

The National Initiative for Cybersecurity Education (NICE) Workforce Framework (NICE Framework) was originally published as NIST Special Publication 800-181 in 2017. NICE has issued several updates regarding the Framework, including draft Task, Knowledge, and Skill (TKS) statements, Ability Statements, and Competency Areas, and a report to Congress, "Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework". The *Cybersecurity Skills Journal* is seeking manuscript proposals that examine the usefulness, benefits, and challenges associated with the adoption, adaptation, or extension of the current NICE Framework, including the draft Competencies and report on measuring capabilities, to improve learning and advance the state of cybersecurity capability maturity.

Submitted abstracts may address any aspect of the NICE Framework, though emphasis should be placed on empirical support for effective awareness, application, and impact of the NICE Framework in enhancing the cybersecurity capability maturity of the entrant, extant, or future workforce, including the cybersecurity practitioner, educator, or researcher. Submissions related to cybersecurity technology or tools should emphasize the human factors involved in the technology design, development, use, or support.

Timeline for the Special Issue: NICE Framework - 2023 Volume

- September 23, 2022: Call for Proposals released
- October 2022: Proposal Development Workshops begin
- October 15, 2022: Submissions opens
- February 15, 2023: Early submission deadline for Articles (prioritized for publication)
- May 15, 2023: Initial Idea submission for Notes and Dialogues close
- July 15, 2023: Final Manuscripts due for September release
- September 15, 2023: Digital release begins

The *Cybersecurity Skills Journal* uses a two-step submission process to encourage submissions aligned with the Journal's mission. Prospective authors are highly encouraged to review our Overview Presentation and attend a proposal development workshop to understand the different paper types and submission requirements. The Manuscript Content Guidelines provides details on what the Journal publishes with specifications for practice, instructional design, or research section manuscripts. Abstracts on technical solutions that lack a substantive contribution for improving or teaching skillful performance of cybersecurity job functions and roles do not align with the Journal's mission and will not be considered.

NATIONAL CYBERWATCH CENTER

Cybersecurity Skills Journal: Practice and Research is published by the National CyberWatch Center. Our authors benefit from exceptional support including but not limited to constructive advice received from 10-person peer review and mentoring panels. Through print and electronic access, articles published in the *Cybersecurity Skills Journal* are available to a global audience of over 400 institutions and 35,000 potential readers. Additional information about *Cybersecurity Skills Journal* is available on the National CyberWatch web page at https://csj.nationalcyberwatch.org.