NICE Community Coordinating Council
Meeting Minutes
March 23, 2022 | 3:30-5:00 p.m. ET

I. Introduction and Ground Rules

NICE Program Manager Susana Barraza opened the meeting, reviewed the ground rules, and reminded everyone that Community Coordinating Council meetings are not for marketing or other promotional purposes. Members are encouraged to participate in the meeting via the platform chat space and type questions in the Q&A space.

II. Opening Remarks

a. Government Co-Chair - Rodney Petersen, Director of NICE

- NICE Director Rodney Petersen welcomed everyone to the call.
- Playbook for Workforce Frameworks
  As NICE developed the 2020 revisions to the Workforce Framework for Cybersecurity (NICE Framework), one consideration was how it could be made more interoperable with other workforce frameworks. They incorporated modularity, flexibility, and agility into the Task, Knowledge, and Skill (TKS) building blocks approach to describing cybersecurity work and the workforce. The building blocks approach sets a foundation for a common framework model. Two other NICE resources, the Task, Knowledge, and Skill (TKS) Statements Authoring Guide for Workforce Frameworks and NISTIR 8355, NICE Framework Competencies, supplement this approach, and together they provide a basis for a common model.

  A Playbook for Workforce Frameworks would include:
  - A Model Framework Structure that contains:
    - Building Blocks: Task, Knowledge, and Skill (TKS) Statements
    - Sample Uses: Competencies, Work Roles, Teams
    - Optional Components: Proficiency Levels, Capability Indicators, Credentials
  - Guidance on how to write TKS statements, competencies, and work roles
  - Workforce framework template
  - Practices for workforce framework development and engagement

III. Standing Items

a. Report Roundup – Learning from Good Ideas

Pre-University Cyber Security Education: Developing cyber skills amongst children and young people
Presented by Virginia Franqueira, Institute of Cyber Security for Society (iCSS)
University of Kent, Canterbury, UK
URL: https://cybilportal.org/publications/pre-university-cyber-security-education-a-report-on-developing-cyber-skills-amongst-children-and-young-people/

- Report Methodology
  - Systemic literature review
  - Desk research based on publicly available online resources

- 21 semi-structured interviews with 24 interviewees to confirm findings and get expert opinions about things not in the public domain.

- 13 Countries Covered in three groups
  - English speaking countries
  - Estonia, Netherlands, Norway, Portugal
  - Greece, Mexico, South Africa
- Key Findings
  - Two main approaches to embedding cybersecurity and online content in the curriculum:
    - Content added as part of a technology subject areas
    - Content added to an array of non-tech subjects
  - Three lacks towards a cybersecurity-related career path
    - Lack of practical cybersecurity skills
    - Lack of security mindset
    - Lack of enough skillset coverage built in
  - A concern was observed across the board regarding lack of teacher training which led to insufficient teaching skills, and teachers struggled with finding enough time to cover cybersecurity content in class.
  - Multiple stakeholders in different sectors are active in different aspects of pre-university cybersecurity education.
    - Activities are often fragmented.
    - Confusion could arise regarding which organization would take the main responsibility.
  - Economics has a direct impact on pre-university cybersecurity education.
    - Teaching traditional subjects is a higher priority.
  - There are different levels of development/maturity of pre-university cybersecurity education in different countries.
  - A top-down approach to curriculum design is the norm adopted across the counties studied, for both formal education and extra-curricular activities.
  - In some countries, teachers and schools have a lot of control over what to teach. This creates freedom and autonomy for teachers, but there are often concerns about a lack of direction.
  - There is a perceived general lack of interest and awareness among children in developing cyber skills and cybersecurity as a potential career path. One key problem is lack of diversity in terms of students' enrolment in optional courses and training events.
- Q&A

  Q: Does the report show an indication that cybersecurity is part of teachers' expectations?

  A: There is a lot of diversion on this issue and a huge range of engagement among teachers.

b. Research Review- Driving Research on Effective Practices

U.S. Cyber Games Data
Presented by Rachel Skillman, Katzcy
URL: https://www.uscybergames.com/

Season 1 Recap:

- Key Dates
  - US Cyber Open – May 28-June 11
  - US Cyber Combine – July 9-September 3: Athletes worked with coaches.
  - US Cyber Team Draft Day – October 5: 20 athletes and 5 alternates were announced.
  - ICC in Athens, Greece: June 14-17, 2022
- Data collected during the Cyber Open
  - 688 people registered across 43 states
  - 328 people completed a first challenge/level
  - 70% male/ 23% female/ 7% preferred not to say
  - 32.6% are people of color
  - 12.5% are US military veterans
  - Three weak areas: cryptography, web exploitation, reconnaissance

Season 2 Preview:

- Upcoming season will be announced in April.
- Will continue to highlight cryptography, forensics, web exploitation, reverse engineering, and reconnaissance.
- Will allow winners in each category.
- Will continue to collect data to monitor trends.

c. Strategy Stories – New Developments that align to NICE Strategic Plan

NIST Privacy Workforce Public Working Group (PWWG)
Presented by Dylan Gilbert, National Institute of Standards and Technology
URL: https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group

- PWWG Origin
  - Problem: Stakeholder were finding challenges with privacy workforce recruitment and development. Demand was outpacing supply.
  - Why NIST? Benefits of NIST Privacy Framework are enhanced with a sufficient pool of skilled and knowledgeable privacy professionals.
- PWWG Goal
  - To support the development of a workforce capable of managing privacy risks by identifying and documenting tasks, knowledge, and skills aligned with the NIST Privacy Framework.
  - This is an interdisciplinary effort involving people from compliance, legal, product design, IT, marketing, etc.
- PWWG Model: NICE Framework SP 800-181 Rev. 1
  - Workforce framework model
  - TKS statement "building blocks"
- PWWG at a Glance
  - 650 members representing the Americas, Europe, Africa, Asia, Australia
  - Short-term project teams, with approximately 50-100 members each, looking at Risk Management/Policies, Processes, Procedures/Data Processing Ecosystem Risk Management
- Lessons Learned

- Identifying the appropriate level of detail or granularity for TKS Statements is challenging.
- Effectively reaching PWWG's broad audience/user base is challenging. The work product must be helpful not only for the privacy workforce, but also for hiring departments and educators.

IV. **Working Group Updates**

a. Promote Career Discovery
Co-chairs: Roland Varriale II, Argonne National Laboratory; Jimmy Baker, Arrow Electronics; Keith Davis, Koinonia Family Life, Inc

- Significant progress has been made on the *Multiple Career Pathways* project, which addresses Objective 1.2 of the NICE Strategic Plan. Three of the five workstreams on this project are complete.
- The working group is also exploring ideas for Cybersecurity Career Awareness Week, to be held October 17-22, 2022.
- Next meeting: April 20, 2022 at 3:30 p.m. ET

b. Transform Learning Process
Co-chairs: Dr. Donna Schaeffer, Marymount University

- There are two active projects:
  - *Improve the Quality and Availability of Credentials*: This team is developing a basic of definition of a credential and determining how to translate competencies versus knowledge in assessments.
  - *Incorporating Cybersecurity into Public Service Education*
- The working group soon will initiate a third project on Learning and Employment Records (LERs).
- Next meeting: April 13, 2022 at 3 p.m. ET

c. Modernize Talent Management
Co-chair: Kevin Perry, United States Army

- The *Cyber Career-Entry Guidance for Job Seekers & Employers* project is divided into two teams, one looking at guidance for employers and the other looking at guidance for job seekers. This project addresses Objectives 3.3 and 3.4 of the NICE Strategic Plan.
- Next meeting: April 21, 2022 at 1 p.m. ET

V. Community of Interest Updates

a. Apprenticeships in Cybersecurity
Co-chairs: Tony Bryan, CyberUp; Debbie McLeod, McLeod Information Systems

- The COI welcomed a new co-chair, Debbie McLeod.
- At the March 25 meeting, there will be a guest speaker from the Department of Labor Office of Apprenticeship, who will discuss the 90-Day Trucking Apprenticeship Challenge, which seeks to promote the apprenticeship model to get more well-trained drivers on the road. The Challenge asks employers to commit to accelerating the development of new apprenticeship programs and expand existing ones.
- Next meeting: April 22, 2022 at 11 a.m. ET

b. Cybersecurity Skills Competitions
Staff Support: Susi Barraza, National Initiative for Cybersecurity Education

- The Summer Social Engineering Event, hosted by Temple University and open to high school, undergraduate, and graduate students, kicks off May 14 with a virtual orientation. The competition will take place on Fridays, Saturdays, and Sundays in May and June.
- The Competitions COI will be changing the day of its monthly meeting. Stay tuned.

c. K12 Cybersecurity Education
Co-chair: Thomas Trevethan, Palo Alto Networks Cybersecurity Academy

- The COI is in the process of refreshing resources and looking at new projects, including activities for Cybersecurity Career Awareness Week.
- Next meeting: April 14, 2022 at 3:30 p.m. ET

d. NICE Framework Users
Karen Wetzel, Manager of the NICE Framework

- The COI conducts its discussions via the mailing list forum. If you have questions, insights, or leading practices to share with the community, join the group today.

VI. Project Progress Reports

a. NICE Conference and Expo (Atlanta, Georgia) – June 6-8, 2022
Presented by Paola Hechavarria, Florida International University
URL: https://niceconference.org/

- Conference Registration: Open until May 16
- Workshop Registration is now open.
- Prevailing government rate is available.
- Preliminary Agenda is available at: https://niceconference.org/agenda/
- Pre-Conference: April 14, 2022

b. NICE K12 Cybersecurity Education Conference (St. Louis, MO) – December 5-6, 2022
Presented by Felicia Rateliff, Director of Operations and Programs, iKeepSafe
URL: https://www.k12cybersecurityconference.org/

- Location: Marriott St. Louis Grand, conveniently located downtown.
- Prevailing government rate of $141/night is available.
- First Planning Committee meeting: March 24, 2022
- Call for speaker proposals will be open from mid-April to late June.
- Early bird registration will open in mid-August and close in late October.
- Live+ format will incorporate some virtual activities, including discussion boards, games, exhibitor booths, etc.
- Sponsorships, which start at $3500, includes both in-person and virtual booths and in-person and virtual exposure and engagement.
- Contact Felicia with questions at: k12cybercon@ikeepsafe.org

VII. Featured Topic

NIST Cybersecurity RFI
Presented by Cherilyn Pascoe, National Institute of Standards and Technology
URL: https://www.nist.gov/cyberframework

- This is a wide-ranging RFI with three main parts:
  - Cybersecurity Framework (CSF): What changes or improvements to the CSF would be useful, especially in light of evolving threats and the evolving landscape. NIST wants to be sure to hear from educational institutions as well as industry and government stakeholders.
  - Cybersecurity Resources: This part seeks feedback on NIST cybersecurity resources, including the relationship of the CSF with other NIST resources and external resources. What can be done to establish further harmonization? They want to look for opportunities for greater alignment among various resources.
  - Supply Chain Cyber: NIST has increased attention on supply chain risk management. How do we address supply chain risk as part of the CSF, and how can NIST broadly address this challenge? They hope to build public/private partnership around this challenge. The RFI seeks feedback on how to scope The National Initiative for Improving Cybersecurity in Supply Chains (NIICS).
- Comments are due April 25, 2022.
- Q&A

  Q: What are the areas of need in the supply chain cybersecurity section?
  A: This is a very open call for information. They want to know what the biggest challenges are and what should they be focusing on next. The community should be driving the conversation. Should there be more work on hardware, on IoT, on open source software?
  Q: How might academic organization find the CSF more useful? (Community College Cybersecurity Summit: Coming up in May https://www.my3cs.org/
  A: The CSF can be used as a training tool. People teaching and training on how to use the Framework often have the best insights on the challenges with it. The academic community has its own cybersecurity interests as well.
  Q: How are the CSF and the Privacy Framework related?
  A: The CSF and Privacy Framework have similar structures. NIST designed the Privacy Framework so it could be used in conjunction with CSF. There had been a lot of concern from stakeholders about incorporating privacy into the CSF itself. They are also looking for feedback on how to make sure the Framework is useable for IT, OT, IoT, etc. It needs to be written at a level that it isn't out of date 5 years from now. Other resources can be used to address specific technologies. For example, NIST just published a profile on ransomware.

VIII. Closing Remarks and Next Meeting Reminder

The next NICE Council Meeting will be **April 27**, **2022** at 3:30 p.m. ET.