NICE Community Coordinating Council
Meeting
July 27, 2022 | 3:30-5:00 p.m. ET

I. **Introduction and Ground Rules** – NICE Program Manager Susana Barraza

- The NICE Community Coordinating Council was established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.
- Members are encouraged to participate in the meeting via the platform chat space and submit questions in the Q&A space.
- Reminder: The meeting it is not intended for marketing or other commercial purposes.

II. **Opening Remarks**

a. Academic Co-Chair – Marni Baker-Stein, Chief Academic Officer and Provost, Western Governors University

- An important topic in academia right now is how to promote short-form credentials to fill needed gaps in the workforce. We should be paying attention to the discussion taking place around the financial aid rules for students pursuing short-form credentials -- aid is not being offered for credentials from online providers. Unfortunately, a conversation that should be about outputs has become a conversation about inputs.

b. Government Co-Chair – Marian Merritt, Deputy Director of NICE

- [National Cybersecurity Education and Workforce Summit:](#) The White House Office of the National Cybersecurity Director (ONCD) hosted a cybersecurity summit July 19 with participants from government, academia, and industry. The summit was co-hosted by the secretaries of Commerce, Labor, Education, and Homeland Security. NIST Director Laurie Locascio participated and offered some important remarks, as did NICE Director Rodney Petersen. There were representatives from higher education, training organizations, and employers. Several organizations made major commitments after the summit.
- A [120-day Cybersecurity Apprenticeship Sprint](#), a joint effort between the Department of Commerce and Department of Labor to create more programs and expand existing programs, was announced at the White House summit. A website was created for both employers and apprentice-seekers. Since the announcement was made, six new apprenticeship programs have been added to the [NICE Cybersecurity Apprenticeship Program Finder](#).

III. **Standing Items**

a. **Report Roundup** – Learning from Good Ideas

2022 (ISC)2 Cybersecurity Hiring Managers Guide
Presented by Tara Wisniewski, EVP Advocacy, Global Markets, and Member Engagement, (ISC) [2]
URL: https://www.isc2.org/research

- After the White House summit, (ISC)[2] announced the [One Million Certified in Cybersecurity](#) program to put 1 million people through its foundational *Certified in Cybersecurity* entry-level certification exam and education program for free.
- The *2022 (ISC)2 Cybersecurity Hiring Managers Guide* discusses best practices for hiring and developing entry- and junior-level cybersecurity practitioners and the benefits of bringing them on board.
  - Creating Job Descriptions: Creating job descriptions should be a shared responsibility among cybersecurity hiring managers, their teams, and human resources. HR often does not understand the roles they are hiring for, and this is leaving hiring organizations and candidates equally frustrated. Collaboration is key. Job descriptions are also a key issue, and there is a need for clarification on technical and non-technical requirements.
  - Top 5 tasks for Cybersecurity Newcomers: For entry-level (with less than 1 year experience) employees, the top five tasks are: Alert & Event Monitoring; Documenting Processes & Procedures; Using Scripting Language; Incident Response; Reporting. For junior-level (with 1-3 years experience), the top five tasks are: Information Assurance; Backup, Recovery & Business Continuity; Intrusion Detection; Encryption; Penetration Testing
  - Time to Train Entry- and Junior-Level Staff: To train entry-level staff, 28% of respondents said it takes 7-9 months, 26% said it takes 4-6 months, and 21% said it takes 10-12 months. To train junior-level staff, 26% of respondents said it takes 4-6 months, 19% said it takes 7-9 months, and 19% said it takes 10-12 months.
  - Typical Cost to Train Staff Before they Can Work Independently: 82% of respondents said it costs less than $5000 to train entry-level staff. 63% of respondents said it costs less than $5000 to train junior-level staff, while 27% said it costs between $5000 and $9,900 to train junior-level staff.
- Q&A
  Q: What was the context when defining entry- and junior-level staff?
  A: It was based on a broad swath of large and small employers, and it included individuals that have at least 25% security responsibility in their job role.

  Q: How many industry responses were there?
  A: There was a respondent base of 1,250 cybersecurity hiring managers from the US, UK, Canada, and India.

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

120-Day Cybersecurity Apprenticeship Sprint
Presented by Kimberly Hauge, Office of Apprenticeship, Department of Labor
URL: https://www.apprenticeship.gov/cybersecurity-apprenticeship-sprint

- The [120-day Cybersecurity Apprenticeship Sprint](#) aims to create more registered apprenticeship programs and expand existing programs. It will culminate during National Apprenticeship Week in the fall.
- Goals
  - Connection: Connect career seekers to RA programs
  - Awareness: Increase awareness of successful RA programs
  - Recruitment: Recruit employers to explore RA
  - Education: Educate the public on the accelerated approach model. Help employers launch programs in as little as 48 hours, which means joining an existing program.

- o DEIA
- Resources
  - o [Department of Labor/Department of Commerce joint press release](#)
  - o [Cybersecurity Apprenticeship Sprint Website](#)
  - o [CybersecurityApprenticeship@dol.gov](#)
- The Department of Labor has received 714 inquiries already in the sprint. More than 100 inquiries are from organizations looking to start programs.
- How You Can get Involved
  - o Help spread the word. If you are interested in supporting an information session, the government will support it. The government is supporting a series of [accelerator events](#).
  - o Refer interested organizations to the sprint website.
  - o Develop a DEIA strategy.
- Q&A
  Q: Are you tracking the levels of apprenticeship completion and what happens to the apprentices afterwards. Are you backing up the sprint with statistics?
  A: The Department of Labor maintains great statistics on apprenticeship programs.

c. **Framework Feature** – Applications and Uses of Workforce Framework for Cybersecurity

The Hiring Manager Role in Successful Cybersecurity Apprenticeships
Presented by Alan Berry, CISO, Centene Corporation

- What Does a Cyber Person Look Like?
  - o Drop your pre-conceived notions: We are not all computer science majors with 4.0 GPAs. There are a lot of talented people who want the jobs but can't even get the initial interviews. You have to open up your aperture.
  - o Cybersecurity talent should be curious, intelligent, eager to learn, diligent, and just a little suspicious
  - o College degrees: Hard requirement or just a suggestion? You have to engage and be active to make sure you put in words what you really need and draw a line between what is required and what is preferred.
  - o Joe the Patch has every security certification offered, but is he any better? You have to balance different factors.
- Cybersecurity Teams: Build or Buy Talent?
  - o The Obvious Answer – A Mix of Both: Building talent is rewarding and changes lives, but it is slow and frustrating. We need to be good corporate citizens. Apprenticeships are a financially responsible way to build teams.
  - o Clearly identify spots for entry-level hires: 50% of teams could be entry level, but small teams may make that difficult.
  - o Create and communicate internal career paths: Internal hires are usually cheaper, get started quicker, and already know whom to call. A clear description of what different jobs and roles require incentivizes your teams. Based on matching NICE Framework work roles to the roles they needed, they were able to establish sample career paths. For example, a sample Threat Intelligence Career Path goes from Jr. Cybersecurity Threat Analyst to Cybersecurity Threat Analyst to Principal Cybersecurity Threat Analyst to Threat Intelligence Manager. This gives employees an idea of a career ladder. It can also show that not every roles starts on the first floor. It shows what someone needs to do to get the role they want.

- Where You Can Find Talent
  - Retained search - expensive
  - Jobsites – not bad, but not really good
  - College interns – if you can define a 10-12 week project
  - Veterans – often already trained and ready to go
  - Apprenticeships – differentiated from internships
  - Contract right to hire – try before you buy

d. **Research Review –** Driving Research on Effective Practices

2021 Social Engineering Event
Presented by Dr. Aunshul Rege, Temple University
URL: https://sites.temple.edu/socialengineering/

- 2021 Summer Social Engineering Event Overview
  - High school, undergrad, grad students from all disciplines
  - Context: Pen Test the CARE lab and its employees
  - Attack vectors: OSINT, phishing, and vishing
  - Pen Test Report
  - Ethics board and risk management vetted the event
  - More information: https://sites.temple.edu/socialengineering
- 2022 SE Event Theme: CARE Lab Hit with Ransomware
- 2023 SE Event Theme: Romance Scams
- Challenge: Deception and Ethics
  - Aren't you teaching students how to deceive others? Isn't what you're doing ethically wrong?
    Response 1: Not teaching this is far worse than teaching it; the best defense is a good offense; ethics and codes of conduct are included.
    Response 2: NICE Framework Success Story. NICE Framework KSAs helped them align with a well-known taxonomy, which makes them more familiar to those who are new to the social engineering space.
    Response 3: DEI; skills equity equals relatability; everyone can try their hand at this; all disciplines are welcomed and valued.
- Lessons Learned
  - Evaluation/assessments (student/educators) and self-reflections are helpful.
  - Meaningful partnerships – nonprofits/government/industry/academia – validate the importance of what they're doing.
  - They need better metrics.

IV. **Working Group Updates**

a. **Promote Career Discovery**
   Co-chair: Keith Davis, Koinonia Family Life, Inc.

- The working group is finalizing a Career Pathways Report.
- They are looking for good examples of people who took alternative pathways into cybersecurity – for example, someone who entered through an apprenticeship program and went directly into a job, or someone who entered through a reskilling opportunity. If you know someone whose journey was unconventional and they are willing to be interviewed, let the working group co-chairs know. The deliverable will be a reference that discusses the multiple pathways and links to the interviews.

- They are also working on a Cybersecurity Ambassador Program. They are brainstorming the structure and want to launch it during Cybersecurity Career Awareness Week in October.
- If you know anyone who would like to be interviewed for the NICE Framework in Focus interview series, email Karen Wetzel: karen.wetzel@nist.gov
- Next Meeting: August 17, 2022, at 3:30 p.m. ET

b. **Transform Learning Process**
Co-chairs: Richard Spires, Learning Tree; Dr. Donna Schaeffer, Marymount University

- The *Improve the Quality and Availability of Cybersecurity Credentials* project team has delivered a report that focuses on articulating a common definition of credentials, developing criteria and processes for identifying the quality of a credential, seeking evidence to document the value of credentials, and increasing the accessibility and affordability of credentials. It includes a one-pager on the value of credentials.
- The *Incorporating Cybersecurity Into A Public Service Education Project* team is working over the summer on background research. They are supported by a professor and his students at Carnegie Mellon University. They are conducting a survey to glean what cybersecurity learning exists in these programs today and will use that as a launching point for making recommendations about how to increase cybersecurity learning in those programs.
- The working group is discussing other projects they might initiate.
- Next Meeting: August 10, 2022, at 3 p.m. ET

c. **Modernize Talent Management**
Co-chairs: Kevin Perry, United States Army; Dr. Melissa Woo, Michigan State University

- The working group's two project teams that are looking at guidance to help employers and job seekers close the gap in expectations both have written draft recommendations. The guidance for job seekers still requires input on how someone can gain experience before they have experience. If you have insights on this, please contact the working group co-chairs or liaison.
- The next project is starting to get teed up.
- Next Meeting: August 18, 2022, at 1 p.m. ET

V. **Community of Interest Updates**

a. **Apprenticeships in Cybersecurity**
Co-chair: Debbie McLeod, McLeod Information Systems
- At their last meeting, the COI discussed:
  o 120-Day Cybersecurity Apprenticeship Sprint
  o Apprenticeship Ambassador Announcement
  o (ISC)[2] 's One Million Certified in Cybersecurity program announcement
- Next Meeting: August 26, 2022, at 11 a.m. ET

b. **Cybersecurity Skills Competitions**
Co-chair: Amelia Phillips, Highline College

- At their last meeting, the COI discussed:
  o US Cybersecurity Games
  o A project compiling a list of all competitions and a way for people to search for them. They have an initial list and want to put it on the website eventually.

- o Finishing two publications on building and running competitions. They to complete these publications by the end of the year.
- Next Meeting: August 18, 2022, at 3:30 p.m. ET

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

- At their last meeting, the COI discussed:
  - o Hacker Shack, a resource for primary school students
  - o National Intern Day: Interns from NICE, NCCOE, and other organizations were invited to speak about their work this summer. The COI asked them about how they learned about cybersecurity concepts and careers and how the community can best market cybersecurity careers. They captured great feedback from their answers.
- Next Meeting: August 11, 2022, at 3:30 p.m. ET

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

VI. **Project Progress Reports**

a. **NICE K12 Cybersecurity Education Conference**, St. Louis, Missouri – December 5-6, 2022
Presented by Felicia Rateliff
URL: https://www.k12cybersecurityconference.org/

- Speaker proposals are in review; acceptances/declines will be emailed August 1.
- Speaker management: Speaker collateral and tasks will be managed through Cadmium Ed Harvester.
- Early Bird Registration and the agenda will be announced August 15.
- Keynotes: Susan Warner, Vice President, Talent Community Engagement, Mastercard; Arica Willis, high school student; Bastian Freund, Special Agent, Cellular Analysis Survey Team, FBI, St. Louis
- Opening Speaker: Dr. Margie Vandeven, Commissioner, Missouri Department of Elementary and Secondary Education
- Cybersecurity Signing Day: Pre-recorded presentation, live entertainment, and Meet & Greet. They are looking for one more student, who is 1) currently in high school, 2) participating or participated in an internship, apprenticeship, or training, and 3) committing to a cybersecurity career.
- They are looking for sponsors and exhibitors. There will be both in-person and virtual booth opportunities. Sponsorships start at $3500.
- Contact Felicia if you have questions: felicia@ikeepsafe.org

b. **NICE Conference and Expo**, Seattle, Washington – June 5-7, 2023
Presented by Randy Pestana, Florida International University
URL: https://niceconference.org/

- The planning committee is discussing themes.
- Timeline
  - o October 3, 2022-January 22, 2023: Call for Proposals – They will be expanding speaking opportunities for next year.
  - o November 16, 2022: RICET, Virtual Pre-Conference Event – an international outreach event looking at best practices in the western hemisphere.

- February 27, 2023-March 19, 2023: Early bird registration
- April 2023: Pre-Conference in Seattle
- March 20, 2023-May 14, 2023: Regular Registration
- May 15-28, 2023: Late Registration (if applicable)
- Email with questions: info@niceconference.org

c. US Cybersecurity Games
Presented by Brad Wolfenden, Katzcy
URL: https://www.uscybergames.com/

- Season II US Cyber Open: Took place July 1-10
  - 9-day Competitive CTF hosted by Virginia Cyber Range
  - Beginner's Game Room offered this year to provide a more introductory experience (not part of the competitive CTF).
  - Registration open to everyone
  - 30+ challenges run out of the US Cyber Games CTF-d instance.
  - 1,470 athletes from 51 states/DC – double the number from last year
  - Most between the ages of 18 and 26
  - 65% male/ 25% female
  - 56% college graduates
  - 46% have professional certifications
  - 19% currently pursuing higher education
- Season II US Cyber Combine: August 4-September 5
  - Kick-Off: August 4 via Zoom: Season II coaches will be announced
  - Invite-only training and evaluation.
  - 100-120 athletes will be invited to the 4-week course.
  - Must be a US citizen, 18–26 years old.
- Season II Draft Day: October 17, Washington, DC
  - The selection of 50 total athletes will be announced.
  - There will be two teams, Stars and Stripes.
- International Cybersecurity Competition: August 2023, San Diego, CA
- Email Brad with questions: wolfendenb@katzcy.com

VII. Featured Topic

Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework
Presented by Karen Wetzel, Manager of the NICE Framework, National Initiative for Cybersecurity Education
URL: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

- NICE is preparing the report in response to an NDAA21 request.
- The report clarifies the difference between proficiencies, proficiency levels, and career levels.
- Example Proficiency Scales: Educational Models; Federal Government Models; Private Sector Models
- Key Characteristics of Workplace Proficiency Scales:
  - Demonstrative: How capability is evidenced
  - Supervision: Amount and type for the level
  - Professional Skills: Soft skills, employability skills

- Proficiency levels will help with establishing career pathways.
- Recommendations
  - Establish a workplace-focused NICE Framework proficiency scale modeled after the SFIA Levels of Responsibility and incorporates criteria of supervision, complexity, professional skills, knowledge, and influence, to be applied to Competency Areas and Work Roles; and develop a stakeholder communication plan
  - Encourage the NICE Modernize Talent Management Working Group to establish a Project Team for NICE Strategic Plan Goal #3: Align qualification requirements according to proficiency levels
  - Engage stakeholders and subject matter experts to develop statements of proficiency to apply to NICE Framework

VIII. **Closing Remarks and Next Meeting Reminder**

The next NICE Council Meeting will be **September 28, 2022**, at 3:30 p.m. ET.