NICE Community Coordinating Council
Meeting Minutes
October 26, 2022 | 3:30-5:00 p.m. ET

I. Introduction and Ground Rules

Danielle Santos, Manager of Communications and Operations and Lead for International Engagement, NICE

- 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 the Q&A space.
- Reminder: The meeting it is not intended for marketing or other commercial purposes.

II. Opening Remarks

a. Industry Co-Chair – Bridgett Paradise, Chief People and Culture Officer, Tenable

- Hearing more about 'quiet quitting' except in cybersecurity. Time to refocus efforts to ensure processes and approaches to hiring and growing talent takes on a longer-term strategy. The current environment enables the ability to strive for real change and grow the workforce.
- The NICE Community Coordinating Council co-chairs wrote a blog on skills-based education and hiring '*Why Employers Should Embrace Competency Based Learning in Cybersecurity'*. It discusses the importance of partnerships between employers, education and training, prioritizing competencies and skills over the use of mandatory degree requirements. The blog looks at how education can close the hiring gap and entice non-traditional candidates through education and sponsorship. It examines how Human Resources can be influenced to revise the current thought process to maximize results for recruiting and hiring.

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

- Please take a look at the blog post '*Cybersecurity Awareness Month 2022: Recognizing and Reporting Phishing'*.
- Cybersecurity Career Awareness Week was last week and many in the NICE Community helped to advance the campaign. Very pleased in the progress over the last year as more people are choosing cybersecurity. It is important to continue to promote the discovery of Cybersecurity Careers throughout the year.
- Rodney participated on a panel as a member of the Maryland Cybersecurity Council. Impressed by the engagement across state-government but also with local business and academic leaders. Getting locals business leaders as well as politicians in state government engaged on these topics is helpful to not only advancing the Cybersecurity Workforce but also the economic development of local communities.

III. **Standing Items**

a. Report Roundup – Learning from Good Ideas
Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

Presented by Inka Karppinen and Jason Nurse, CybSafe
URL: https://www.cybsafe.com/whitepapers/cybersecurity-attitudes-and-behaviors-report/

- Ran a large-scale survey with key project partners form the US, the UK and Canada. Explored five security risk behaviors to find out how people perceive these security behaviors, their attitude with respect to these security behaviors and how they actually behave on a day to day basis. The behaviors were selected based on guidance from NIST, National Cybersecurity Alliance (US), the National Security Center (UK) and GetCybSafe (Canada). The core five behaviors of focus were: 1.) Ensuring password hygiene, 2.) Applying Multi-Factor Authentication (MFA), 3.) Installing the latest updates 4.) Checking emails for signs of phishing and 5.) Backing up data
- Findings:
    - 62% of the sample said they had no access to training. Only 14-16% of survey respondents had access to training.
    - Majority of respondents reportedly attended a yearly mandatory training, as opposed to ongoing security training. Additionally, they were required to complete training when something went wrong, like a cybersecurity breach at work. Common training topics covered were recognizing phishing emails and how to use a strong and separate password.
    - Reported barriers to training included lack of time and thinking they already had enough knowledge about cybersecurity.
    - Training impact was good. More than half said they were better at recognizing phishing messages. 45% have started to use strong passwords. 40% of respondents said they use multi-factor authentication (MFA). Half of the participants reported cybersecurity training as useful.
- What can you do? Explain the why. Why creating good passwords comes before how to do it. Explain the benefits of MFA and why it adds layers of security. Explain how being safe online helps save time, money and nerves. Must provide clear and usable guides and tools.
- It is important to support the younger generation who tend take cybersecurity for granted.
- Q&A:
  Q: How has your thinking evolved and how is your instrument helping to demonstrate the difference between awareness vs. behavior? How have you observed that action being implemented over time?
  A: Awareness by itself does not change behavior. Need to think about the perspective of the person. Security is secondary thinking to a focus of productivity. Need people to understand that security is helping job performance and not a hindrance.
  Q: Are you seeing technological advances have impact?
  A: Yes, substantial impact as it is no longer a block to productivity. Simple things like biometrics allows an individual to implement authentication so that they don't need a password, or have to enter a pin every time they use a device.
  Q; How does your research or questions interest people in cybersecurity careers by making security easier?
  A: We describe the barriers for good cybersecurity behavior. Someone in IT who does not apply MFA may not have a cell phone, for example. Or, an individual's perception of the topics improve after training.

b. Strategy Story – New Developments that align to NICE Strategic Plan
The Search for the Cyber Unicorn

Presented by Sasha O'Connell, Executive in Residence & Director, THSP MS Program
Department of Justice, Law and Criminology, American University
URL: https://cyberflorida.org/

- A pilot study explored the question of whether the persistent cybersecurity workforce gaps are exasperated by employers setting unattainable expectations of new hires looking for both work experience and relevant education to come in at the entry level?
- Employers indicated previous work experience was more important than education in this context. In a related finding, respondents indicated experience requirements are often wish lists requiring more than is necessary for the role, but 56% of the employer responses indicate those requirements are realistic. Hiring managers are primarily responsible for determining the job requirements.
- Great engagement from the employers but challenges with collecting data from students which left a gap in the methodology.
- Q&A:
  Q: When will the results be publicly available or published?
  A: The results will likely come in the next few months.
  Q: Any indication from employers about what was most important and desirable?
  A: Preliminary findings show that it is job experience.
  Q: Do you have a hypothesis as to the low student participation?
  A: There were technical challenges and students took advantage of the mechanism. Also looking at better times of year to conduct the survey. Comes down to faculty engagement at the classroom level to encourage students to participate.
  Q: Would employers accept experience from competitions in lieu of work experience?
  A: Anecdotally, it has had a huge impact getting them over the hump with employers.

c. Framework Feature – Applications and Uses of Workforce Framework for Cybersecurity
NICE Framework: maximizing success in Commercial Enterprise
Presented by Jason Swope

- The NICE Framework is critical to businesses futures. Commercial Enterprise business practices would help accelerate growth opportunities. NICE customer segments consist of government, contracting and commercial enterprise. In government and contracting, the government is the customer. The Office of Personnel Management and contracting officer representatives are the targeted stakeholders respectively. In commercial enterprise it's a different beast. The Government is not the customer and executive or business leader stakeholder engagement must speak the language of business financials.
- Leverage senior executive services, ECQ4, business acumen to speak the language of commercial enterprise business financials. In commercial enterprise, the NICE value proposition must present strategically with executives, operationally with HR and tactically with employees to get full acceptance and support in private industry. There is value proposition in HR for recruitment and retention and to employees in career options.
- The NICE Framework is critical in business futures especially if government wants to maximize public-private collaboration and engagements. Government must treat commercial enterprise as the customer and speak the language of business.
- Q&A:
  Q: Can you elaborate on the type of individuals for whom the value proposition would be directed?
  A: All individuals. Employees are looking for job opportunities that are not necessarily in

cybersecurity if they are already in it. They are frustrated they don't have a CISSP and are looking for other options like knowledge manager, intelligence officer, risk manager. Show cybersecurity practitioners these other options so they stay with their organization which saves on recruitment and retention. Entice the C-SUITE to learn about cybersecurity, policy and planning. There are other jobs like policy advisor, policy and planning, etc. Point students and employees toward the National Initiative for Cybersecurity Careers and Studies (NICCS) Cyber Career Pathways Tool. They can explore what interests them both personally and professionally. Show and maximize the framework first value proposition by explaining that the core KSAs and tasks taught in cybersecurity can be transferred to any business unit.

IV. **Deeper Dive**

Incorporating Cybersecurity Into A Public Service Education Project Team
Presented by Andrew Artz, NIST and Stacy Drudy, NASPAA
URL: https://www.nist.gov/document/public-service-education-project-naspaa-ncaec-introductionspdf

- The Network of Schools of Public Policy, Affairs, and Administration (NASPAA) is a non-profit membership association with over three-hundred schools in both the United States and abroad. NASPAA graduates primarily go to work in government.
- Initially had four critical questions: 1.) How is cybersecurity currently taught in NASPAA programs? 2.) What are the potential opportunities and challenges facing programs who wish to incorporate cybersecurity throughout their curricula? 3.) What are the TKS statements that describe what a graduate must know about cybersecurity on "day zero" of their professional career? 4.) How do we bridge the gaps between where the programs are to where students need to be?
- Major tasks were completed to answer these questions:
  - Request for Information (RFI): took syllabi from professors in NASPAAs programs and mapped them to cyber knowledge units as well as the NICE Framework.
  - Performed a SWAT analysis looking at the opportunities and challenges that would face NASPAA organizations if they incorporated cybersecurity into their programs.
  - Semi structured interviews with employers and alumni.
  - Coordinate curriculum to match the needs of the workforce
- This is an issue that needs to be solved in NASPAA's program. There are challenges in that NASPAA credits these individual degrees. Students will think that if they want to take a cyber course they will have to go into a college for engineering or information technologies. Found those courses are not appropriate for NASPAA students. Topics such as the Presidential Policy directives, FISMA or what OMB does are typically missing in colleges of engineering or IT. There are several schools that have moved early into cyber curriculum, such as Carnegie Mellon and American University. There are several programs that have developed an extension course or concentration but few programs with a cyber policy focus.
- Draft recommendations: The project team has looked at equipping NASPAA students with a basic understanding of cybersecurity appropriate to their graduate placement. Secondary objective would be to provide pathways into cyber if graduates want to become more technical. Recommend NASPAA integrate cybersecurity throughout existing programs and curricula as an elective. An alternative could be for NASPAA programs to enrich or develop service model's reciprocity agreements between programs in order to send students for an elective course virtually.

- Q&A:
  Q: In your review of programs have you discovered programs that are targeted toward executive leaders?
  A: The concentration has been on NASPAA students not executive leaders. The recommendations that this become a part of core classes would reach leadership students who are mid-career and in the executive education programs.
  Q: Why is it important to the NASPAA membership to create cybersecurity offerings?
  A: The recommendations that this become a part of core classes would reach leadership students who are mid-career as well as the executive education programs. Implementing these classes is important for the NASPAA students as 53% of them go into government and will need to be prepared for cyber-attacks. Being educated in cybersecurity is essential to helping people make policy decisions.

V. **Working Group Updates**

a. Modernize Talent Management
Co-Chair providing update: Lynsey Caldwell, Leidos

- The group conducted updates to and a review of their environmental scan.
- Joined by two guest speakers on the last meeting. One from Leidos discussing a new initiative, Leidos Life, focused on employee careers, flexibility and well-being. The second, a professor from the University of Arizona, spoke about resources the Higher Education Information Security Council (HEISC) offers to employers at higher education institutions and/or the security program partnership with University of Arizona's cybersecurity programs, creating internship opportunities to add hands-on experience, preparing students for future careers.
- Kicking off a new project to write *An Employers Guide to Writing Effective Cybersecurity Job Descriptions.* Looking to for a project lead.
- Site: Modernize Talent Management Working Group | NIST
- Next meeting: November 17, 2022 at 1:00 p.m. ET

b. Promote Career Discovery
Co-Chair providing update: Keith Davis, Koinonia Family Life, Inc

- Celebrated Cybersecurity Career Awareness Week (CCAW) with a special panel presentation on non-traditional pathways to enter a career in cybersecurity. The speakers shared about both traditional and non-traditional pathways to prepare those entering the cybersecurity workforce. Webinar was well received and attended.
- Site: Promote Career Discovery Working Group | NIST
- Next meeting: November 16, 2022, at 3:30 p.m. ET

c. Transform Learning Process
Co-Chair providing update: Richard Spires, Learning Tree

- Kicking off two new projects: 1.) Create a resource guide for employers to provide information on free and low-cost training modules and programs, for building a diverse and inclusive cybersecurity workforce and, 2.) Look at products and service companies to support efforts to have performance-based assessments to measure cybersecurity competencies.
- The projects will work to identify best practices, products and services available across the industry and make those more known to the community.

- Transform Learning Process Working Group | NIST
- Next meeting: November 9, 2022, at 3:00 p.m. ET

VI. Community of Interest Updates

a. Apprenticeships in Cybersecurity
Co-Chair, Debbie McLeod, McLeod Information Systems

- The October meeting takes place Friday, October 28, 2022 at 11:00 a.m. ET. Sean McGowen of ThriveDX will speak about how their training platform aligns with the NICE Framework.
- Discussions on what the next project will be are ongoing.
- Site: Apprenticeships in Cybersecurity Community of Interest | NIST
- Next Meeting: October 28, 2022, at 11:00 a.m. ET

b. Cybersecurity Skills Competitions
Lead: Davina Pruitt-Mentle, NICE

- The Competitions COI celebrated CCAW with a special presentation on the value of cybersecurity competitions which took place during the regular monthly meeting.
- Site: Cybersecurity Skills Competitions Community of Interest | NIST
- Next Meeting: November 17, 2022, at 3:30pm ET

c. K12 Cybersecurity Education
Co-Chair, Thomas Trevethan, Palo Alto Networks

- Kristi Rice and students from Spotsylvania High School discussed how they celebrate (during their career spirit week) and shared about activities and events that have proven successful in promoting careers in cybersecurity. The student panel also discussed their plans for after high school graduation.
- Site: K12 Cybersecurity Education Community of Interest | NIST
- Next Meeting: November 9, 2022, at 3:30 p.m. ET

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

- New staff member, Caron Carlson, has joined the NICE staff in support of the NICE Framework.
- The final NICE Framework Competency Areas NISTR will be out in the next month or so which will include the new list of competency areas for member feedback.
- Finalizing knowledge and skill statements. Expect them to be final this year as well.
- Site: NICE Framework Users Group | NIST

VII. Project Progress Reports

a. Cybersecurity Career Awareness Week – October 17-22, 2022
Presented by Davina Pruitt-Mentle, NICE Lead for Academic Engagement
URL: https://www.k12cybersecurityconference.org/

- Over 500 events and commitments and over one-hundred thousand people impacted.
- The social media challenge show-cased examples of how people are engaging in CCAW.
- The week started with a kick-off event, Opening remarks from Congressman Langevin. The event informed attendees about the efforts taking place around workforce development.

- Attended the US Cyber Games after the kick-off event; a Capture the Flag competition was held by the Virginia Cyber Range; The Department of Education announced their two Presidential Cybersecurity Educator of the Year Awardees (from CA and OH).
- The next CCAW is the week of October 16-21, 2023. Thanks to everyone who participated.

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/

- Early bird registration is open until October 31, 2022 and the fee is $275. The General registration fee is $350.
- Fee for Federal employees is $275 through December but it does not include meals.
- There are 13 pre-conference workshops over December 3-4, 2022. Registration for the pre-conference workshops will open on October 7, 2022. Each 120-minute workshop is $75.
- Few rooms are left in the hotel block for $141/night at the Marriot.
- Opening Speaker: Dr. Margie Vandeven, Commissioner, Missouri Department of Elementary and Secondary Education.
- 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
- Program includes: Fireside chat with recently announced cybersecurity teacher award winners for 2022; 8 break-out sessions in 5 tracks; exhibitor showcase; capture the flag; multiple games including virtual and in-person formats and a Beer and Bread Boarding Social on Monday night.
- Panels: School Counselor Panel will include counselors from the American Schools Counselor Association. A Student Panel will consist of six students ranging from eighth grade to high school talking about their stories.
- Cyber Signing day-mini event: the event will feature 7 students currently or have recently participated in an internship and or apprenticeship program.
- Sponsorship and Exhibiting Opportunities: still a few spots available for on-site exhibitor tables. Email: K12cybercon@ikeepsafe.org
- Email Felicia Rateliff with questions: felicia@ikeepsafe.org

c.) NICE Conference and Expo (Seattle, WA) – June 5-7, 2023
Presented by Paola Hechavarria, Cybersecurity Coordinator, Florida International University
URL: https://niceconference.org/

- Conference theme: 'Resetting Expectations: Creating Accessible Cybersecurity Career Pathways'
- Call for proposals: October 3, 2022 - January 22, 2023. Submit proposals to: https://niceconference.org/proposals/.
- RICET, Virtual Pre-Conference Event: November 16, 2022: Regional Initiative for Cybersecurity Education and Training (RICET): hosted by OAS and FIU and supported by NICE. It is a virtual and free event. Additional information can be found here.
- Early Bird Registration: February 27, 2023 – March 19, 2023; Regular Registration: March 20, 2023 – May 14, 2023; Pre-conference event in Seattle, WA: April 2023 (est); Late Registration (if applicable): May 15 – May 28, 2023
- Visit https://niceconference.org/sponsors/ for information about sponsorship opportunities.
- The Westin Seattle room block is open: https://niceconference.org/hotel-travel/

- Connect with us:
  - Website: www.niceconference.org
  - Email: info@niceconference.org
  - Twitter: @nicecybercon
  - NICE Conference Linkedin Group: https://www.linkedin.com/groups/12696840/

d.) Cyberseek.org
Presented by Randi Parker, Senior Director, Partner Engagement for CompTIA Spark
URL: https://www.cyberseek.org/

- CyberSeek has 2.5 million unique views since launching. Expect to cross 3 million in Q3 of next year.
- Employers listed more than 769,000 openings, positions or jobs requiring cybersecurity skills for a twelve-month period ending in September 2022. Employer demand for cybersecurity grew 2.4 times faster than the overall rate across the US economy. Slight pull back in hiring activity recently. However, cybersecurity hires were up thirty percent more in Q3 2022 over the previous year. The supply and demand job ratio held steady. There are approximately 65 cybersecurity workers in the job market for every 100 jobs.
- Requirements for cybersecurity skills for specific occupations have increased dramatically over last 12 months. Cybersecurity professions are expanding into other fields.
- Cyberseek's grant was renewed for another three years.

e.) US Cyber Games
Presented by Jessica Gulick, CEO, Katzcy
URL: https://www.uscybergames.com/

- During the US Cyber Games Open, candidates submitted an application for consideration for a special invite to a combine. The US Cyber Combine is a virtual eight-week session: 4 weeks of intense evaluation followed by four weeks of engagement on soft and core skills and tech talks.
- On October 16, 2022, Season II coaches were brought in for a summit and held a draft to select the Season II team. Different values were taken into consideration in determining the final thirty players.
- Monday, October 17, 2022: US Cyber Games Draft Day
  - 422 registrations
  - 154 In person attendees
  - 946 online views which grows about 100 views every day.
  - Two keynote speakers: Kevin Stine, Chief, Applied Cybersecurity Division, NIST and Nitin Natarajan, Deputy Director from CISA
  - Announced 30 team players over the course of two hours.
  - 23 pipeline players nominated and will get training and mentorship opportunities to strengthen them for next year.
- Additional Info can be found here: https://www.uscybergames.com/events
- Hosting the International Cybersecurity Championship from July 30-August 4, 2023.

VIII. Research Review- Driving Research on Effective Practices

Interagency Roadmap to Support Space-Related STEM Education and Workforce
Presented by Quincy Brown, Senior Policy Advisor, Office of Science and Technology Policy (OSTP)

URL: https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Interagency-Roadmap-to-Support-Space-Related-STEM-Education-and-Workforce.pdf

- The work focuses on equity and the STEM ecosystem. The first Space Council meeting was held December 1, 2021. Vice President Harris announced the US Space priorities framework. The key themes in the framework include space exploration, space science, the commercial space sector, climate change, national security and STEM. OSTP was charged with two tasks: use space to inspire more students to be interested in stem as well as identify the barriers to entering and staying in the space workforce. OSTP developed a plan of action including the establishment of the Space STEM taskforce. The task force is focused on three areas:
  - 1.) Inspire greater engagement from educators and learners in space-related STEM content and fields
  - 2.) Prepare educators, training providers, learners, and job seekers through experiences that support the transition into the space workforce
  - 3.) Employ a diverse workforce to bring the benefits of space to more communities
- The White House released a fact sheet including federal and private sector commitments that align with the Space STEM focus areas and goals.
- Aggregated K-12 Space STEM educator resources and career guides:
  - K-12 Space STEM Resources
  - Space Career Guide

IX. Featured Topic

National Apprenticeship Week
Kimberly Hauge, US Department of Labor
URL: https://www.apprenticeship.gov/national-apprenticeship-week

- National Apprenticeship Week is November 14-20, 2022. It is the culmination of the 120-day apprenticeship sprint. There will be a number of events.
- Apprenticeship Week celebrates apprenticeship throughout the country. Visit the site for more information as well as to register any events or to get materials.
- There will be a key theme for every day of Apprenticeship week.

X. Closing Remarks and Next Meeting Reminder

The next NICE Council Meeting will be **Wednesday, November 30** at 3:30 p.m. ET.

**Reminder – we are combining our November and December meetings. If you still see the originally scheduled November 23 or December 21 meeting on your calendar, please delete it. Please reach out to the NICE Program Office for any calendar assistance.*