# NICE Community Coordinating Council
## Meeting Minutes
### April 23, 2024 | 3:30-4:45PM ET

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

   a. 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.
   b. Members are encouraged to participate in the meeting via the platform chat space.
   c. Reminder: The meeting is not intended for marketing or other commercial purposes

II. **Opening Remarks**

   a. Industry Co-Chair – Michael Alicea, Chief Human Resources Officer, Trellix

      i. In light of the rise of AI, education and training is still critical to workforce preparation.
      ii. AI is creating opportunities for automation, but those automated processes are, in turn, opening up new requirements for cybersecurity.
      iii. We have to keep pace with, if not surpass adversaries who are using AI.

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

      i. NICE Conference will feature a plenary session on AI.
      ii. This year's monthly webinar series from NICE began with looking at demographics across the US and seeking to focus on underserved and underrepresented communities that can help us close the cybersecurity workforce gap. Upcoming webinars include communities such as justice-involved individuals, youth, and refugees.

III. **Featured Content**

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

   *Cleared for Success (CFS)*
   Presented by Bill Britton, Vice President for Information Technology, Chief Information Officer, and Director of The California Cybersecurity Institute, California Polytechnic State University, San Luis Obispo
   URL: https://ucm.calpoly.edu/news/cleared-success-cal-poly-announces-unprecedented-cybersecurity-workforce-development-program

      i. CFS aims to connect students with the national mission set of cybersecurity.
      ii. The University saw the opportunity to create a program to serve as an introduction to the defense industrial base complex – what it does and why.
      iii. The CFS program highlights those from the community who can relate to students and who represent a diverse population of people.
      iv. There are three stages of CFS

1. Cultivate student interest and recruitment.
   a. For example, introducing students to the SF 86 form, paperwork that is required to fill out if you are undergoing a background investigation, typically to obtain a security clearance.
   b. Discussions about personal choices, for example: what to keep in mind when applying for a security clearance, how to retain a clearance, and how to interact with people after obtaining a clearance.
2. The development of a secure space to allow students to get stared on opportunities with clearances. Students will experience seeing what it's like working in closed, sensitive, and secure working environments.
3. Development of large-scale security operations.
   v. The program will help students be "day one ready."
   vi. The CFS program is starting with only Cal Poly students. However, the University is thinking about how they could expand to the California State University system (400,000+ students).
   vii. Q: Do you have recommendations for how the federal government can do a better job of onboarding recent graduates and engaging them in real work without them being in that "holding tank" waiting for their clearance to process?
   1. The federal government needs to start their recruiting processes much earlier. If students don't have a job by the winter semester their senior year, they're worried about getting a job. The federal government is slow to reach students. Federal recruiters need to start reaching out to students between their 3rd and 4th year – not their last year when it's too late.
   viii. Q: Thoughts around getting student interns cleared to be able to work in term employment.
   1. Phase 3 of the CFS program aims to address this. With a larger-scale security operations program, students can get pre-cleared (in essence) and employers can use the program to "tap" students to work of projects in the secured environment.
b. Report Roundup – Learning from Good Ideas

   *Bits, Bytes, And Loyalty: How To Improve Team Retention*
   Presented by Yameen Huq, Director of Cybersecurity, Aspen Institute
   URL: https://www.aspendigital.org/report/bits-bytes-loyalty/

   i. Over the past year, the Aspen Institute has observed that "workforce retention" kept coming up as a topic interest and priority.
   ii. The report highlights root causes, symptoms, and real solutions for tackling the retention problem.
   iii. Symptoms found included: turnover, burnout, and limited growth.
   iv. Root causes found included: overwhelming workloads, outdated retention methods, and career stagnations.
   v. Solutions include: the ability to give back and ability to deploy skills, through things like rotational programs.

      vi.    Call to action – a sequence of steps for employers who are designing a retention program. The steps include actions to include assessments, leadership buy-in, implementation, collecting feedback, and refinements and expansion.

      vii.   The report concludes with case studies from companies who have implemented retention programs.

     viii.   Q: In what ways if any, were there recommendations that the working group considered to be unique to the cybersecurity workforce?

         1.   There is a demand for service opportunities and mentorship. Employees seem to want to seek out opportunities to gain hands on experience and demonstrate their skills.

      ix.   Q: While strategies to retain employees are generally good workplace practices, is "retention" a realistic goal when employees can diversify their skills and experiences by moving among different organizations? Similarly, are employers "committed" to retaining and developing employees for the life of their career?

         1.   If everyone relieves the burden of upskilling, then no one is doing it. The cost of losing talent is something to keep in mind. Employers can retain talent by offering certifications and paths for upskilling.

      x.   Q: Has the need for child care been identified as a need to retain employees?

         1.   Yes, health and wellness offerings are a key part of the plan. Workplace flexibilities are important.

      xi.   Q: To what extent was diversity addressed in this report?

         1.   There is a section on the benefit of supporting marginalized groups. There is a unique need in retaining different perspectives in a workplace.

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

*CyberSTAR*
Presented by Christopher Will, Director of Commercial Solutions, WillCo Tech
URL: https://www.willcotech.com/products/cyberstar/

      i.   CyberSTAR provides a framework for compliance to DoD 8140, which supports the Department of Defense Cyber Workforce Framework.

      ii.   The CyberSTAR compliance platform helps people transition from a certification model to a knowledge and skill-based model.

      iii.   Q: NIST takes a risk management approach to cybersecurity, including the NICE Framework as well as "human risk management" for cybersecurity awareness. A lot of people are skeptical of "compliance" as an activity vs "risk management" as a more effective outcome. Does your tool only stress "compliance" or does it take an outcomes-based approach to securing enterprises?

         1.   Christopher will follow up with the product team and report back with an answer.

      iv.   Q: I have experienced that many employers don't really understand the skills/levels of a cybersecurity portfolio. Can we also adapt the compliance to developing hiring matrix?

          1. Part of the roadmap includes identifying the skills that people need to move into different roles in cybersecurity.

IV. **Community Progress Reports**

    a. **Working Group Update**

        i. Promote Career Discovery
Co-chairs: Karl Cureton, Council Exchange Board of Trade (CEBOT)

          1. The new project charter "Effective Practices to Identify, Track, and Measure Cybersecurity Career and Discovery Programs" is [now available](#) online.

          2. The project's primary purpose is to refine the approach to identify, catalog, and evaluate cybersecurity career discovery programs while implementing evidence-based practices.

          3. The project objectives include curating a comprehensive database of current programs, establishing metrics for evaluation, and developing a resource hub for sharing successful practices. The aim is to enhance collaboration among stakeholders and broaden the appeal of cybersecurity careers to a diverse audience.

          4. Website: [https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council/promote-career-discovery](https://www.nist.gov/itl/applied-cybersecurity/nice/community/community-coordinating-council/promote-career-discovery)

          5. Next meeting: May 15, 2024, at 3:30 p.m. ET

    b. **Project Progress Reports**

        i. NICE Conference and Expo (Dallas, Texas) – June 3-5, 2024
Presented by Cesar Cebot, Florida International University
URL: [https://niceconference.org/](https://niceconference.org/)

          1. Registration closes on May 14$^{th}$ or until sell out. Regular conference registration rate is still available.

          2. A limited block of discounted rooms is available at a prevailing government rate of $164/night (room rate does not include tax or any applicable fees).

          3. Pre-conference workshops spots are still available. Register [here](#).

          4. The NICE Conference & Expo agenda is [now available](#).

        ii. NICE K12 Cybersecurity Education Conference (San Antonio, Texas) – December 9-10, 2024
Presented by Felicia Rateliff, iKeepSafe
URL: [https://www.k12cybersecurityconference.org/](https://www.k12cybersecurityconference.org/)

          1. Call for proposals is now open through Thursday, June 11, 2024. Call for proposals consists of breakout session presentations, breakout session panel, pre-conference workshop, and pre-recorded on-demand sessions.

          2. Key dates:

             a. Thursday, May 28 - Planning Committee Meeting

             b. Tuesday, June 11 - Call for Proposals closes

             c. Mid-July - Proposal accept/decline email notifications

          d.    Early-August – Agenda and registration go live

       3.    Contact information: Felicia Rateliff, [K12Cybercon@ikeepsafe.org](mailto:K12Cybercon@ikeepsafe.org).

## V.    Featured Topic

**a.**  *Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development*
Presented by Rodney Petersen, Director; Danielle Santos, Manager of Communications and Operations; Bria Bennett, Research Associate, NICE
URL: https://www.nist.gov/itl/applied-cybersecurity/nice/community/ramps-communities

      i.    RAMPS emphasizes the importance of regional alliances and partnerships involving various stakeholders such as schools, colleges, universities, employers, and economic organizations.

      ii.    RAMPS highlights the focus on meeting employers' needs at state, local, and regional levels, premised on the Department of Commerce's principles for effective workforce investments and good jobs principles.

      iii.    RAMPS applicants were expected to address NICE strategic plan goals and adhere to Department of Commerce characteristics, including employer-led efforts, involvement of multiple community partners, consideration of wraparound services, and emphasis on diversity, equity, inclusion, and earn-and-learn models.

      iv.    Additionally, there needed to be a focus on connecting workforce development to economic development through coordination among federal government efforts and the utilization of private sector or foundation funding to match government funding.

      v.    In 2026, the NICE Program Office launched the RAMPS pilot funding five organizations to support the work they do in their community to support cybersecurity education, training, and workforce development.

      vi.    Due to the positive result of the 2016 pilot, NICE received additional funding to support community-based cybersecurity workforce development initiatives. Eighteen new initiatives were funded earlier this month.

      vii.    The NICE Program Office currently is accepting proposals for a second round of RAMPS funding, for an additional 15 awards. The deadline to submit a proposal is May 24, 2024, at 11:59pm ET. Learn more here.

      viii.    Each award will be funded up to $200,000.

      ix.    Eligibility extends to any nonfederal entity. It is encouraged for a diverse mix of educators, including K-12, higher education, training providers, and employers, along with involvement from private industry and state or federal partners (though federal partners cannot be applicants). Collaboration with community workforce development organizations and nonprofits is also encouraged.

      x.    The performance period for each award is up to two years.

xi. Detailed requirements for applications, including alignment with strategic goals, diversity, equity, inclusion, accessibility, and regional focus, were covered in the Applicant's Webinar which is [now available](#) online.

xii. Proposal content should align with strategies outlined earlier, focusing on local jobs, utilization of the NICE framework, addressing local workforce needs, and establishing multistakeholder partnerships.

xiii. Participation from local organizations through letters of commitment is required.

xiv. Additional resources:
1. [2024 RAMPS Notice Of Funding Opportunity (NOFO) Announcement](#)
2. [Grants.gov RAMPS NOFO Application Information](#)
3. [RAMPS Programs](#)
4. [NISTIR 8287: A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce](#)
5. [Frequently Asked Questions](#)

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

The next NICE Community Coordinating Council Meeting will be **May 28, 2024,** at 3:30PM ET.

**Upcoming Meetings:**

- [NICE K12 Cybersecurity Education COI](#): May 9, 2024, 3:30-4:30PM ET
- [NICE Apprenticeships in Cybersecurity COI](#): May 10, 2024, 11:00-12:00PM ET
- [NICE Cybersecurity Career Ambassadors COI](#): May 10, 2024, 1:00-2:00PM ET
- [NICE Diversity and Inclusion COI](#): May 10, 2024, 2:00 – 3:00PM ET
- [NICE Transform Learning Process WG](#): May 14, 2024, 2:00-3:00PM ET
- [NICE Promote Career Discovery WG](#): May 15, 2024, 3:30-4:30PM ET
- [NICE Modernize Talent Management WG](#): May 16, 2024, 1:00-2:00PM ET
- [NICE Cybersecurity Competitions COI](#):  May 24, 2024, 2:00-3:00PM ET

**Upcoming Events:**

- [NICE Webinar Series](#)
  - [Reintegrating Justice-Involved Individuals into Cybersecurity Careers](#) April 30, 2024, 2-3PM ET
  - [Equity Strategies in Youth Apprenticeship Programs and Partnerships](#) May 8, 2024, 2-3PM ET
  - [Empowering Refugee Communities in Cybersecurity Roles](#) June 12, 2024, 2-3PM ET
- [Youth Apprenticeship Week](#): May 5-11, 2024
- [34th Annual FISSEA Conference](#): May 14-15, 2024
- [NICE Conference & Expo](#): June 3-5, 2024, Dallas, Texas
- [Cybersecurity Career Week](#):  October 14-19, 2024

- [National Apprenticeship Week](): November 18-24, 2024
- [NICE K12 Cybersecurity Education Conference](): December 9-10, 2024, San Antonio, Texas
- NICE Events [Calendar]()