

NICE Community Coordinating Council

Minutes

January 27, 2021 | 3:30-5:00 p.m. ET
BlueJeans Online Conferencing Platform

I. Introduction and Ground Rules

- a. NICE Program Manager Susana Barraza welcomed the community to the meeting and offered an overview of the council, its mission, and its goals. She encouraged everyone to use the Chat space to participate in the discussion.
- b. Slides shared with presentations at this meeting are available on the NICE Community's shared drive:

https://drive.google.com/file/d/1i4Xn4d_6bRLPOgtp6hzdF723ivXi_dY3/view?usp=sharing

II. Opening Remarks

- a. Industry Co-Chair Jon Brickey, Senior Vice President, Mastercard offered some opening remarks.
- b. Government Co-Chair Rodney Petersen, Director of NICE, briefly reviewed the new meeting platform and asked members to provide any feedback on their experience following the meeting. He reminded everyone that NICE is driven by the NICE Strategic Plan, which was recently updated, and the structure of the working groups reflects the plan's goals.

Cybersecurity is a bipartisan issue and not politically polarizing. Workforce and job-related issues are also bipartisan, and it shouldn't be surprising that these are continuous messages from one administration to the next. With the new administration in place, NIST and NICE are undergoing leadership changes. There will be a new NIST director, yet to be named, in addition to a new Secretary of Commerce and many other new officials at the department. During the confirmation hearing of Commerce Secretary nominee, Governor Gina Raimondo of Rhode Island, the cybersecurity workforce and the roles that NIST, NICE, and the NICE community play were mentioned. Rodney said he remains encouraged about NICE's purpose and mission and the work being done by the community.

III. Standing Items

- a. **Strategy Stories - New Developments that Align to NICE Strategic Plan**

Talent Attraction Strategies

Presented by Drew Repp, Content Manager, Community Insights, Emsi

URL: <https://www.economicmodeling.com/2020/08/07/build-dont-buy-solving-the-cybersecurity-talent-shortage/>

- Company Overview

Emsi's work involves connecting job seekers and students with educational institutions and employers, using data, including labor market and skills data. They conduct research in a variety of areas, including talent attraction and development.

They recently produced a *Talent Attraction Scorecard*, which ranks communities and counties according to a variety of metrics, including net migration, job growth, skilled job growth, educational attainment, and annual job openings per capita. They realized that communities need strategies to improve their rankings and produced the *Talent Attraction Strategies for 2021* guide. They released a set of strategies categorized into five phases, ranging from the near term to the long term. For cybersecurity, the strategies mostly fall in the 6 months – 4 years category and focus on transferrable skills, technical programs, and certificate programs.

Last summer, they looked at the skills gap in cybersecurity and found that, nationally, the cybersecurity demand is twice as great as the supply. Demand is greatest in Washington, D.C., followed by New York City, Baltimore, Dallas, Atlanta, Chicago, Virginia Beach, San Jose, San Diego, and Los Angeles. Regional markets vary in the skills needed most, and there are skills clusters. In Detroit, for example, the skill cluster leans towards automotive skills.

- Report: *Build (Don't Buy): Solving the Cybersecurity Talent Shortage*

Organizations seeking to fill a cybersecurity role typically post the job and receive 40-50 applicants, who most likely are employed somewhere else. Basically, they have to buy the talent, but if they need to hire multiple roles over a long period of time, this is not a cost-effective method. There are common career areas that transition into cybersecurity, and it makes more sense to look within an organization's IT and finance departments and then offer training in cybersecurity. They have the underlining skills that transfer to cybersecurity, and micro credentialing or short-term training can build the necessary additional skills.

- For more information, visit: www.economicmodeling.com/research

- Q&A

Q: How much of the skill cluster data is overlapping?

A: None. All of the posting data is deduplicated.

b. Report Roundup - Learning from Good Ideas

White Paper: *Planning for the Future Through Workforce Development*
Presented by Gabriela Montes de Oca, Cybersecurity Program Officer,
Organization of American States

URL: <http://www.oas.org/es/sms/cicte/docs/White-Paper-Cybersecurity-Education.pdf>

- Cybersecurity Skills Shortages in Latin America

Latin America has experienced great transformation over the past year. Because of the pandemic, the region is reliant on the Internet for basic operations, work, school, socializing. At the same time, there has been an increase in the number of malicious activities affecting the region, which was already a target of online attacks. In Latin America and the Caribbean, the cost of cybercrime in 2017 was estimated at between 0.28% and 0.57% of the region's GDP.

The region is lacking 600,000 jobs to meet the necessary requirements for the threats they are facing. The key issue is that cybersecurity education offerings in the region are behind, and COVID-19 showed that they still have a long way to go.

- Report: *Cybersecurity Education: Planning for the Future through Workforce Development*

Last year, the OAS released the *Cybersecurity Education: Planning for the Future through Workforce Development* report. The report outlines steps to build a Cybersecurity Education Action Plan (CEAP), including mechanisms to integrate cybersecurity education into policy development and school curricula. It also offers a toolkit of initiatives and mechanisms at the national level to generate interest in cybersecurity careers.

- National Cybersecurity Policies

Thirteen countries in Latin America have put in place a national cybersecurity policy. Four countries, in particular, have recognized the importance of education in the development of the cybersecurity workforce: Argentina, Brazil, Chile, and Colombia.

- Cybersecurity Education Action Plan (CEAP)

The OAS partnered with NICE to develop the CEAP, which is a blueprint for policymakers to design public policies that will strengthen their national cybersecurity strategies and develop the cybersecurity workforce. Four principles are important to highlight:

- Participation of academia and the private sector at the beginning of the formulation of the framework
- Importance of establishing governance rules and coordination mechanisms
- Elaboration of a strategic plan
- Standardization of the language used in the workplace and in the academic environment.

There are five critical steps for creating a CEAP following the NICE Framework: Establishing Goals, Integrating Stakeholders into the plan, Establishing Objectives and Metrics, Implementing a Cybersecurity Education Plan, and Actionable Recommendations to make the plan a reality.

The Participation of academia and the private sector at the beginning of the formulation of the Framework

- Importance of establishing governance rules and coordination mechanisms
- Elaboration of a strategic plan
- Standardization of the language used in the workplace and in the academic environment

- Workforce Development Lifecycle

The report offers information on things to consider in implementing a CEAP in each phase of the workforce development lifecycle in addition best practices from around the globe. In addition to covering elementary and secondary school, it looks at post-secondary and apprenticeship programs, internships, continuous training and certifications. It also provides information on cybersecurity research and development and building a culture of cybersecurity.

- Other OAS Cybersecurity Initiatives

- Cyberwomen Challenge: A flagship program that teaches women how to face cyberthreats in a contained environment
- OAS-Cisco Academy composed of courses on cybersecurity essentials
- Citi Foundation “creating a cybersecurity career path” and Citi Lab – for children from economically constrained environments
- Cybersecurity Innovation Fund
- Cybersecurity Courses with FIU

- Recommendations

The OAS recommends a national approach to education and cybersecurity and promotes tailored solutions at every stage of the workforce development lifecycle. It also recommends:

- Clear and defined goals to prioritize and integrate cybersecurity education at all levels to guide the actions of policy makers
- Multi-stakeholder approach
- Monitoring mechanisms and indicators that assess progress towards the goals of the action plan.

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

Update on the Federal Cybersecurity Workforce Coding Effort
Presented by Jodi Guss, Human Capital Strategist, Office of Personnel Management

- Federal Cybersecurity Workforce Assessment Act

Much of the work OPM has done in applying the NICE Framework is grounded in the Federal Cybersecurity Workforce Assessment Act, which was enacted in 2015. The act required OPM to: 1) assign new cybersecurity codes aligned to the NICE Framework to positions requiring performance of IT, cybersecurity, or other cyber-related functions; and 2) identify and address critical cybersecurity skills needs.

- Identify positions performing cybersecurity functions through a coding system

In January of 2017, they issued Government-wide guidance on assigning new cybersecurity codes that aligned to the Work Roles described in the NICE Framework. Later that year, agencies issued internal guidance on assigning new cybersecurity codes to positions, and then shared service providers reprogrammed agency systems to accommodate larger data field for cybersecurity codes. In April of 2018, agencies reviewed positions and assigned new cybersecurity codes.

- Identify critical cybersecurity skill shortages through workforce planning

OPM issued Government-wide guidance for determining cybersecurity “Work Roles of Critical Need,” which are the greatest skill shortages in the most critical areas, in terms of Work Roles, in April of 2018. One year later, agencies determined and reported their cybersecurity Work Roles of Critical Need, causes for the shortages, and action plans, targets, and metrics to mitigate the shortages.

- Ensure we have critical cybersecurity skills

Since April of 2019, agencies are supposed to be implementing plans to address their cybersecurity Work Roles of Critical Need and reporting their progress annually.

- NICE Framework

The NICE Framework helped OPM in completing the requirements spelled out in the act. There are a lot of occupations that perform cybersecurity functions. Applying Framework helps hiring managers, CIOs, and other staff partner better in managing the cybersecurity workforce. They have to bring together their expertise to grow and manage the federal cybersecurity workforce. The Framework is also helping them internally talk about cybersecurity work in a much more standardized way. Because of the law, they have had to focus on basic workforce planning. They pinpoint skills shortages and put a priority on budgeting for the, recruiting.

The effort is taking place at the level of agencies and departments focusing on their own work roles and also at a government wide level with pilot programs and programs for interagency details, and reskilling.

IV. Working Group Updates

Rodney offered a high-level overview of the working groups, pointing out that each one focuses on a specific goal in the NICE Strategic Plan. The working groups will conduct environmental scans, identify gaps where new projects or initiatives are needed, and identify strategies and tactics. They will also be working on developing metrics to measure progress.

a. Promote Career Discovery

Co-chair Jimmy Baker, Account Coordinator at the California Cybersecurity Institute, announced that the group's co-chairs met on Monday. They are in an exploratory and ideation phase. Everyone on the team has worked with youth, from middle school to high school and college.

Co-chair Roland Varriale II, Cybersecurity Analyst at the Argonne National Laboratory, said he is looking forward to receiving feedback from the group as they start to move forward with their work.

Rodney added that the working groups will announce the dates and times of their monthly meetings soon.

b. Transform Learning Process

Co-chair Dr. Aurelia T. Williams, Interim Vice Provost for Academic Administration at Norfolk State University, introduced herself. She noted that she is part of a consortium of 13 HBCUs that have changed the opportunities for students to earn cybersecurity degrees and transform them into jobs.

Co-chair Richard Spires, Principal at Richard A. Spires Consulting, introduced himself and noted that he has worked in IT and cybersecurity for the last 30 years and has served in government, including at DHS. He worked on a number of issues in workforce development while in government and has been a

proponent of leveraging the NICE Framework. The working group has not met yet but will soon.

Noting a question in the Chat as to whether this group's work would involve competencies, Rodney said that is definitely a relevant topic for them to address.

c. Modernize Talent Management

Co-chair Kevin Perry, Chief of Cyber Training at the DoD Cyber Crime Center/Cyber Training Academy, introduced himself and reported that co-chairs met recently to discuss the group's work ahead.

The next meeting is scheduled for Thursday, February 18, 2021, at 1 p.m. ET.

V. Community of Interest Updates

a. NICE Framework Users

Karen Wetzel, Manager of the NICE Framework, announced that the new Framework Users Community of Interest was unveiled earlier in the day. The group is meant to be an open space for communication, where users can share questions, insights, and support for applying the Framework in various settings.

b. Apprenticeships in Cybersecurity

Co-chair Tony Bryan, Executive Director of CyberUp, reported that the Apprenticeships group met the previous Friday and discussed the challenges that 2020 brought about, what worked successfully, and what didn't. They talked about what the group can do in the coming year to help drive workforce development through apprenticeships. Tony asked everyone in the group to ask one employer to join them. They are always looking for new members.

c. Cybersecurity Skills Competitions

Co-chair Amelia Phillips, Cybersecurity and Forensics BAS Lead at Highline College, said the group's co-chairs met the previous week to discuss plans for the coming year. Last year they completed two guidebooks, *How to Build and Run a Competition* and *Guide for Competitors*.

The next meeting is scheduled for Thursday, February 18, 2021, at 3:00 p.m. ET.

d. K12 Cybersecurity Education

Co-chair Laurin Buchanan of Secure Decisions said the K12 group met on January 13 and discussed the revised NICE Strategic Plan and the changes involved in transitioning from a working group to a community of interest. They are discussing how the K12 implementation plan and the COI's charter need to be updated to better align with the revised NICE Strategic Plan.

Co-chair Terrance Campbell, CTE Cybersecurity Teacher in Shelby County Schools, introduced himself. He is involved in the launching a high school virtual

cybersecurity internship that will take place this coming summer. He invited input from the apprenticeship group. They want to be sure they can collect data points and see how the model can be replicated.

The K12 COI's monthly meetings this year will be held month on alternating Wednesdays and Thursdays.

The next meeting is scheduled for Thursday, February 11, 2021, at 3:30 p.m. ET.

VI. Project Progress Reports

a. NICE Conference and Expo

URL: <https://niceconference.org/>

Randy Pestana of Florida International University reported that the program committee for the 2021 NICE Conference and Expo met recently and discussed potential themes, tracks, and keynote speakers. If anyone is interested in serving on a committee, contact the NICE program office.

The 2021 conference will be held in Atlanta, and the dates will be announced in February. If you are located in Georgia, consider getting involved in the Georgia Academic Consortium or the Georgia Industry Consortium. The conference organizers are eager for local support. Contact them at:

info@niceconference.org

For more information on the conference or to subscribe to the distribution list, visit www.NICEconference.org

b. NICE K12 Cybersecurity Education Conference

URL: <https://www.k12cybersecurityconference.org/>

Davina Pruitt-Mentle, Lead for Academic Engagement at NICE, reported on the success of the 2020 virtual K12 Cybersecurity Education Conference, which drew more than 700 attendees plus more than 200 students – record attendance. There were more than 100 speakers and numerous keynotes, panels, and tracks, including the first-ever student track.

Attendees commented that, despite the virtual environment, they were able to network, and teachers were able to share stories and strategies. There were discussion boards, birds of a feather, virtual meet-ups, chat spaces, games, prizes, a capture the flag competition, and a National Cyber Signing Day virtual presentation.

The National Cyber Signing Day presentation and the student tracks are available on the conference website to view for free in memory of Randy Ramos, who recently passed away. Randy had established the mechanism for more than 200 students to attend the conference free-of-charge and attend a separate track created just for them.

The rest of the conference content will be available to attendees through 2021.

Save the Date: The 2021 NICE K12 Cybersecurity Education Conference will take place December 6-7.

c. **Centers of Academic Excellence (CAE) in Cybersecurity Community**

URL: <https://www.caecommunity.org/>

Tony Coulson of California State University, San Bernardino, announced that the next CAE National Cybersecurity Virtual Career Fair will take place September 17, 2021. They are targeting colleges and universities in the CAE program. There were nearly 2000 participants at last year's virtual fair, and organizers expect attendance to be even broader this year. They look forward to having many industry partners.

At the next NICE Community meeting, CAE will unveil some of the events and workshops they will be co-sponsoring with NICE over the next year or so.

VII. Closing Remarks

Academic Co-Chair Marni Baker-Stein, Chief Academic Officer and Provost at Western Governors University, introduced herself and gave a brief overview of WGU.

- Western Governors University

Western Governors University is a nonprofit organization founded in 1997 by 19 U.S. governors, with more than 130,000 full-time students. It is made up of four colleges offering more than 60 degrees in high-demand fields, including K-12 teacher education, health professions, business, and IT. The courses are competency-based, and WGU works closely with industry to determine the competencies that are needed. The courses are 100% online and affordable, based on flat-rate tuition per term.

WGU was created to increase access to educational pathways that are aligned with the future of work and to empower individuals for lifelong success. They work from a student-centric model, focusing on programs rather than individual courses and build out programs as full pathways aligned with workforce needs and personalized assessment.

One of the faculty roles is mentor, who helps make sure a student plans each term against reality of their lives – full-time jobs, family commitments, etc. Course instructors work with students to establish an individualized plan of attack to optimize their time. Evaluators provide a blind evaluation of performance to make sure they offer rich, individualized feedback.

- Covid-19 Student Impact Monitor

The faculty serve as a safety net for many of the students as they move through the programs. During the past year, WGU developed a Covid-19 Student Impact Monitor, which mapped the difficulties students experienced because of the pandemic, such as lost jobs, caring for family members, and home schooling. A large percentage of the students are low-income and they have experienced challenges over the past year. The faculty can help with emergency funding, access to computer equipment, and internet access.

They use open skills libraries to match their curriculum with skills and they plan to so that other universities can access and add to them.

- Open Skills Network

WGU partners with a large array of businesses and higher education institutions on the [Open Skills Network](#), which is a convening of organizations interested in skills-based hiring. They are establishing Rich Skills Descriptors as the standard syntax for structured skills data. Each program at WGU is a playlist of competencies defined using industry data, and they want to review each competency and tag them to rich skill descriptors. They have mapped out 10,000 rich skills descriptors. For cybersecurity, the skills are tied to metadata around the NICE Framework.

They are also working on a national network of open and proprietary skills libraries. This spring, they will sponsor alliances around open skills libraries in health, teaching, and 21st century skills. They hope to have an alliance around cybersecurity as well.

VIII. Next Meeting Reminder

The next NICE Community meeting is scheduled for Wednesday, February 24, 2021, at 3:30 p.m. ET.