NICE Community Coordinating Council
Meeting Minutes
April 26, 2023 | 3:30-5:00 p.m. ET

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

- 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 is not intended for marketing or other commercial purposes.

II. Opening Remarks

a. Interim Academic Co-Chair – Paul Bingham, Vice President and Dean, College of Information Technology, Governors University

- Artificial Intelligence (AI) is the hot topic at RSA this year, such as large language models and the way our adversaries are weaponizing them. Conversely, how can AI tools help us protect and defend against attacks? The opportunity to conduct full-scale simulations using AI is now available within the prevention space. AI models can be trained to run simulations to help with prevention.
- Paulo Alto Networks first coined the phrase, 'XDR' for Extended Detection and Response back in 2018. Endpoint Detection and Response (EDR) is becoming XDR. Incorporating AI into all into XDR is allowing the cybersecurity professional to have a holistic view of what is happening at the end point and throughout the network.
- Hearing a lot about authentication methods. Multi-factor authentication (MFA) methods are still important but the attacks against MFA are increasing. Authentication continues to be a challenge to stay ahead of the techniques and tactics that people are using to try and foil those.

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

- Overall, both the focus of the NICE Framework and of the NICE Program is on the security of all things in cyber space. Rodney is reminded while working at the National Institute of Science and Technology (NIST) that the labs about AI, are usually about the security of AI. The work on the Internet of Things (IoT) is about the security of IoT. The focus of NICE and the NICE Framework is about the security of those processes and the privacy as well.

III. Standing Items

a. Report Roundup – Learning from Good Ideas

Future Directions: 2022 Summit Report
Presented by Corrinne Sande, NCyTE Center, Whatcom Community College
URL: https://www.ncyte.net/home/showpublisheddocument?id=271

- Corinne presented about the action planned developed out of the 'The Role of Community Colleges in Cybersecurity Education: Future Directions Summit' back in 2022. Several groups at the summit advised on the strategy. Five strategies were developed. Corinne shared some strategy highlights.
- Strategy 1: Diversify the Workforce. There were several suggestions around this strategy and Corinne shared two of the most practical. First, continue the Scholarship for Service (SFS) program for community colleges but change the program so that students could make their obligation by serving at municipalities, state and local or tribal government. The second, continue the Junior Research Officer Training Corp (JROTC) Program that Whatcom has been hosting but with the change for universities to grant credit to JROTC students that complete a course of study. It primes them to go into the field when they complete high school.
- Strategy 2: Cybersecurity Education provided to K12. There were several points highlighted. The most important was to create a cyber-endorsement for high school educators. The idea is to have a College of Education at a University add an endorsement to the education program that is approved by the superintendent of public instruction. When high school teachers graduate out of their program, they are already endorsed in cyber. Currently working on this with Eastern Washington University but it can be expanded nationwide.
- Strategy 3: Increase Capacity of Cybersecurity Education at Community Colleges. Faculty shortage is an issue across the board. One suggestion is look at who qualifies as faculty. There are qualified people who have 20 years' experience in cyber but may not have a PHD.
- Strategy 4: Expand Business and Industry Engagement and College Program Responsiveness. Improving the community college brand was a noteworthy point. There is a lack of understanding about community colleges graduates. A major part of community college is workforce. There are workforce programs designed to graduate students after two years that can go to work. This is where most of the cyber programs are found. The students all have applied skills. Educate the public on who is graduating from the community colleges that have the skills. Make employers aware of this employee pool. Additionally, improve diversity in hiring and reconfigure job descriptions to expand the pool of applicants. It is about matching the qualifications to actual needs. Corinne has been advocating for standardizing the data about Community College Cyber programs and aligning it. The NICE Workforce Framework has all these work roles and there is need for people in certain work roles. No one really knows who is graduating that could fill that need. A standardization of the data is necessary. Then, one can see there is a shortage of x amount of people for job z. Increase the number of programs that can meet that work role. This will require a better picture of the data.
- Strategy 5: Encourage Government Coordination, Involvement and Support. More collaboration between government agencies was recommended. Also recommended, create a National Initiative with Authority to Direct Cybersecurity Initiatives Across Agencies.
- Q&A:
  Q: Who determines the qualifications requirements for a community college faculty member?
  A: It is a combination of what the overall requirements are at the college, which

have changed over the years. It used to be a combination of work and education or workforce programs. There has been a trend toward valuing education over work experience. It's determined by the college and in alignment with whatever the accreditation standard says.

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

Retaining Women through Register Apprenticeships and Women in Apprenticeship and Nontraditional Occupations (WANTO) Grants
Presented by Kimberly Hauge, US Department of Labor
URL: https://www.dol.gov/newsroom/releases/wb/wb20230414
https://www.apprenticeship.gov/investments-tax-credits-and-tuition-support/open-funding-opportunities

- The Department of Labor's Women's Bureau is issuing its Women in Apprenticeship and Nontraditional Occupations (WANTO) Grants. This funding opportunity will help address significant underrepresentation of women, in registered apprenticeships, in skilled trade, manufacturing and healthcare. Women make up only 14 percent of registered apprentices while they account for nearly half of the labor force.
- DOL will issue five million to fund six to fourteen projects ranging from $350,000 to $750,000 with a twenty-four-month period of performance. To be eligible for funds, an applicant must be a community-based organization. The closing date for the applications is May 29, 2023.
- The program aims to provide technical assistance and pointers, which may include public or private sectors, labor unions and tribal territories in the United States to encourage employment of women in both principle and non-traditional occupations by developing programs and providing orientations and setting up support groups.
- The second request for proposals is one on expanding registered apprenticeships through industry intermediary contracts. It is advertised on Apprenticeship.gov. It is labeled 'Tier 2: Registered Apprenticeship Acceleration in Established Industries RFP'. It specifically targets expansion of registered apprenticeships in cybersecurity along with hospitality and trucking. This RFP seeks to work with industry intermediaries to work within established industries with an existing registered apprenticeship (RA) presence and the demand/capacity to accelerate and scale further growth and expansion to quality RA for all workers. The duration of performance is twelve months with three twelve-month options. Applications are due May 18, 2023. Link: https://www.apprenticeship.gov/investments-tax-credits-and-tuition-support/open-funding-opportunities

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

MasterCard and the NICE Framework
Presented by Katie Boudreau and Bonnie Leff, MasterCard

- MasterCard has begun to include the NICE Framework in various ways within their cybersecurity area. MasterCard had an engagement with CyberVista to help build their workforce mapping of fifteen of their roles within corporate security. They have identified framework competencies that align with those fifteen roles.

- They have utilized that information along with additional feedback from their hiring managers, to begin including NICE competency proficiencies and related work roles into their job descriptions and additional job description enhancements.
- MasterCard is looking for more ideas and assistance moving forward. How can they include the NICE Framework and NICE work roles in other ways into what they do at MasterCard? Hope to find a more granular way to find the KSAs that line up to those competencies.
- Q&A:
  Q: Have you incorporated this at all levels of roles MasterCard is posting for at this point?
  A: Yes, for the last few months they have been including the piece about the NICE Framework references into all their corporate security roles that have been posted. Everything from entry-level to VICE President.
  Q: How do you think this has improved your alignment of candidates with the actual work roles?
  A: They don't have any metrics on that yet.
  Q: Do you have any measurements you intend to put into place to see whether using this is working?
  A: Yes, they do have plans to include some training enhancements and some other evaluations into the NICE Framework and referrals.

d. Research Review- Driving Research on Effective Practices

The State of Inclusion Women in Cybersecurity
Presented by Paolo Gaudiano, Aleria Tech
URL: https://www.wicys.org/wp-content/uploads/2023/03/Executive-Summary-The-State-of-Inclusion-of-Women-in-Cybersecurity.pdf

- A joint project was created between Aleria PBC and Women in Cybersecurity (WiCyS) to understand why the representation of women in cybersecurity is not where it should be.
- Launched a pioneering study to gain insight into the causes of disparities in cybersecurity that keep women from being recruited, retained, and advanced.
- Why is this pioneering and what is unique about it? When most people talk about DEI, the focus is on the 'D'. Aleria understands the need to look at all the factors that makes a person want to go to a job and stay in it. They have developed a unique way of measuring inclusion called an inclusion assessment. An inclusion assessment is a workshop where they educate people on a unique way of thinking about inclusion and how it links with diversity and the performance of the organization.
- Aleria has gone through Phase 1 with WiCyS.
  - They conducted an inclusion assessment of individual women (mostly WiCyS members) to establish the value of the approach and identify initial insights.
  - They collected anonymous data and asked people to share experiences about when they felt uncomfortable in the workplace.
  - They also asked two questions about their experiences. The first, what category of experience was it (such as work life balance, respect, career advancement, etc.). They also asked about the source. In phase one they collected data from over 300 women who were individual members.
- They have just started phase 2.

    - They are conducting additional inclusion assessments for WiCyS strategic partner organizations, to provide data and insights for each organization and create a robust industry-wide benchmark.
- The experiences that were shared were ranked by categories. Respect was the most prevalent category. Career and Growth was ranked second.
- Most workplace experiences result from interactions with leadership, direct managers, and peers. People, not policies are the most common sources of experiences of exclusion.
- Women working for WiCyS partner organizations report much lower levels of exclusion. Additional analysis suggests that WiCyS programming targets the most impactful "Categories of Inclusion."
- Paolo Gaudiano: paolo@aleria.tech

IV. Working Group Updates

a. Promote Career Discovery
Co-chairs: Jimmy Baker, Arrow Electronics

- A presentation was provided by Sara Shrieve from Cisco on Corporate Social Responsibility.
- Jimmy presented on the FBI's Internet Crime Complaint Center (IC3) report on cyber-attacks.
- Received an update from the NICE Framework Team.
- Received an Ambassador Program Update.
- Provided working members a link to a document to review the group's goals and objectives.
- Site: Promote Career Discovery Working Group | NIST
- Next meeting: May 17, 2023, at 3:30 p.m. ET

b. Transform Learning Process
Co-chair: Richard Spires, Richard A. Spires Consulting

- Currently have two active projects and both will be showcased at the upcoming NICE Conference.
- Next meeting, the group will join the K12 COI. One topic of discussion will be around the strategic plan objective 2.6, focusing on championing the development of recognition of teachers, faculty, and instructors as part of the in-demand workforce.
- Searching to replace Richard Spires as co-chair. If interested, please reach out through the NICE team.
- Site: Transform Learning Process Working Group | NIST
- Next meeting: May 10, 2023, at 2:00 p.m. ET.

c. Modernize Talent Management
Susana Barraza, NICE

- Guest speaker, Karen Wetzel, spoke about the NICE Framework. She shared about competency areas and how they differ and can be used with the work roles. She also previewed an upcoming release expected this year.
- An update was provided by the 'Guidance on Writing Effective Job Descriptions' project team. The team is currently working on a workshop with the goal to bring

hiring and talent acquisition managers together to hear about what works and what makes sense from their perspective. Be on the lookout for additional information.

- Site: Modernize Talent Management Working Group | NIST
- Next meeting: May 18, 2023, at 1:00 p.m. ET

V. Community of Interest Updates

a. Apprenticeships in Cybersecurity
Co-chair: Katie Adams, Safal Partners

- Recently held a webinar with Robert Half International, which has a National Apprenticeship Program for several tech occupations. Great opportunity for attendees to learn more about the intermediary model of apprenticeship.
- Next month the group will hear from Drexel University, which recently received apprenticeship program approval from the Pennsylvania State Apprenticeship Agency.
- The group completed their COI survey. The top area of project work interest is in developing and deploying a survey to determine industries, both current and future, projected cyber occupational needs for apprenticeship. The COI would also be interested in identifying new occupations for consideration for DOL approval. There is also significant interest in drafting a white paper on methods of implementing apprenticeship at various talent levels.
- Site: Apprenticeships in Cybersecurity Community of Interest | NIST
- Next meeting: May 12, 2023, at 11:00 a.m. ET

b. Cybersecurity Skills Competitions
Co-chair: Amelia Phillips, University of the Cumberlands

- The group had two presentations. One, the Atlantic Council, presented on their Cyber 9/12 Strategy Challenge. It is an annual cyber policy and strategy competition where students from across the globe compete in developing policy recommendations tackling a fictional cyber catastrophe. The second presentation was on the ICL Collegiate Cup and the International's Cyber League America's Cup.
- An update was provided about the website the group has been creating to track all competitions. It will be a dynamic database.
- Site: Cybersecurity Skills Competitions Community of Interest | NIST
- Next meeting: May 18, 2023, at 3:30 p.m. ET

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

- Heard an announcement about the Mathematics and Statistics Awareness month.
- An expert in cybersecurity education and artificial intelligence (AI) presented on the potential benefits of using Chat GPT in cybersecurity education as well as the challenges and risks associated with this technology.
- Project updates were provided for the K12 Conference, the Ambassadors Program, and the Cybersecurity Awareness Month.
- Next meeting will be in collaboration with the Transform Learning Process Working Group.

- Site: K12 Cybersecurity Education Community of Interest | NIST
- Next meeting: May 10, 2023, at 3:30 p.m. ET

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

- Proposed changes to the NICE Framework were released this week for comment involving the Work Role categories and Work Roles.
- There is an introduction and summary. The team wants to be very clear and detailed on the reason why they are being proposed and the impact they might have. There is a full description of the changes. Additionally, the changes being made are listed in a spreadsheet that people can review. The comment period closes on June 23, 2023.
- The proposed changes address earlier community feedback (both from comment periods as well as from workshops, working groups, community calls, and other stakeholder conversations).
- Some changes include adjusting the Work Role titles to resemble actual Work Roles instead of appearing like job titles. For example, instead of the role being defined as Enterprise Architect, it was updated to Enterprise Architecture. Want to be clear a work role is not the same as a job title.
- Ensure that there is alignment with other frameworks. One example, the Department of Defense Cybersecurity Workforce Framework (CWF), where they have Intelligence and Cyber Space Effects as their categories would have aligned to the NICE Frameworks' Analyze and Collect and Operate categories. Changing the titles of those categories and making sure the work roles are in the same order as the CWF. Also looking at how these ties in alignment with other areas. Ensuring that the language is not too government speak. Using language that will be well understood in all areas.
- Work Role Category Names: The changes are to better represent the work being conducted within those categories and make them more descriptive. Securely Provision becomes Design and Development. Operate and Maintain becomes Implementation and Operation. The categories now designate a body of work rather than a verb itself. Protection and Defense become Protect and Defend. Oversee and Govern become Oversight and Governance. Oversight and Governance is moving to the top of the category list. The team is proposing to delete the 'Investigate' category and move the work roles elsewhere.
- Work Role Name Changes: The category description changes are to primarily improve consistency and clarity. Replacing "IT" and "information technology" with just "technology" to reflect the broader environment for cybersecurity work. Replacing the word "or" with "and" in a category description. Also adjusting work role names to better reflect standard language.
- Work Role Deprecations: There is a new work role, which is being called 'Systems Developer'. Content from this role is merged into Information Systems Security Developer to create the updated Systems Development Work Role. Similarly, when looking at the Law Enforcement/Counterintelligence Forensics Analysis work role, redundancies with two existing work roles were found. Content from this role (7 statements) is merged into Cyber Defense Forensics Analysis to create the updated Digital Forensics Work Role. The Cybercrime

Investigation Work Role (previously "Cyber Crime Investigator") description is updated to reference language from the Law Enforcement/Counterintelligence Forensics Analysis Work Role.

- The team wants to hear feedback from the community. Once the comment period closes, the team will look at how the feedback can be addressed in the proposed changes.
- Q&A:
  Q: Will the Cyber Seek Heat Map be updated to reflect these changes?
  A: The team has been in conversations with Cyber Seek. A lot of planning in how to do that. Also working on a process documentation of release and versioning schedules. There will be a process for this in a consistent manner. Next month they will release an updated competencies list for comment. Following, around the NICE Conference, the team will release their updated knowledge and skill statements.

VI. Project Progress Reports

a. NICE Conference and Expo (Seattle, Washington) – June 5-7, 2023
Presented by Susana Barraza, NICE
URL: https://niceconference.org/

- The NICE conference is June 5 - June 7, 2023, at Westin Seattle in Seattle, Washington.
- Regular Registration is open and they expect a full sell out. March 20 – May 14, 2023. https://niceconference.org/hotel-travel/
- Encourage registration for the pre-conference workshops. They are expected to sell out. The workshops will be held on Monday, June 5, 2023, from 1-5:00pm PT.
- Book your hotel: The Westin Seattle: Hotel & Travel - NICE | Conference and Expo (niceconference.org).
- A local stakeholder pre-conference event took place on April 3, 2023, in Seattle, Washington. A recording is available online.
- Thanks to the 2023 sponsors and key partners. Sponsorship opportunities are sold out.
- Connect with us:
  - Website: www.niceconference.org
  - Email: info@niceconference.org
  - Twitter: @nicecybercon

b. NICE K12 Cybersecurity Education Conference (Phoenix, Arizona) – December 4-5, 2023
Presented by Felicia Rafeliff, iKeepSafe
URL: https://www.k12cybersecurityconference.org/

- The NICE K12 Conference will take place December 4 – December 5, 2023. Pre-conference workshops will be on Saturday, December 2, 2023.
- The conference will be at the Hilton Phoenix Resort at the Peak and government rates will be available until November 10, 2023. Registration is now live.
- The first planning committee meeting was last month. It is a long process for creating the conference theme. This year there is a new promotion for the conference, 'Cybersecurity Careers…It's What's Hot!'

- Call for Proposals opens on April 27, 2023, and close on July 14, 2023. They will have submissions for pre-conference workshops, breakout sessions, panels, pre-recorded sessions, and virtual poster sessions. Get on the mailing list!
- The theme for the presentation is, "Designing K12 learning experiences to build a diverse and skilled cybersecurity workforce."
- The five tracks this year are: 1.) Increasing Cybersecurity Career Awareness 2.) Engaging Students Where Disciplines Converge 3.) Stimulating Innovative Cybersecurity Educational Approaches 4.) Promoting Cybersecurity Career Pathways and 5.) Promoting Cyber Awareness
- Actively recruiting sponsors and exhibitors at many different financial levels. Great opportunity to represent your organization at the conference.
- The 2023 pre-conference workshops will be held at Grand Canyon University. A tour will be provided as well as hands-on activities.
- Connect on Twitter:
  - @ikeepsafe
  - NISTcyber
  - #NICEK12

VII. Featured Topic

NIST Cybersecurity Framework 2.0
Presented by Cherilyn Pascoe, National Institute of Standards and Technology
URL: https://www.nist.gov/cyberframework

- The NIST Cybersecurity Framework (CSF) provides guidance to organizations to manage cyber security risks. It was originally an Executive Order directive and congressional mandate to develop a set of best practices to reduce risk to critical infrastructure.
- The CSF does not indicate 'how' to address outcomes, or 'which' outcomes are higher priority. The cybersecurity framework uses more passive language focused on the outcome statements. The NICE Framework uses more active language.
- The Cybersecurity Framework has become widely used by all sectors around the world and helps to translate cybersecurity topics across technical teams and non-technical teams. Organizations use the framework to report on their cybersecurity posture to senior executives within an organization, as well as discussions outside of an organization with suppliers and customers and among various government agencies.
- The framework was last updated five years ago in 2018 with only a minor update. NIST put out a request for information (RFI) last year and asked if the Cybersecurity Framework should be updated. They majority of respondents said that while the framework is still currently affective to address cybersecurity risks people also want many changes to be made common. Thus, NIST decided to move forward with a major update.
- The goal is to have a final publication of CSF 2.0 in early 2024. The community has been engaged throughout the process to ensure they are addressing the specific risks organizations are facing. The framework should be effective and easier to adjust.
- NIST has published many frameworks in the technology and cybersecurity space. The update gives NIST the opportunity to increase alignment with other resources and frameworks. The NICE Framework, the Privacy Framework, the AI Risk Management Framework, and the Secure Software Development Framework should all remain separate frameworks. They all provide valuable guidance to their audiences. However, they want to increase alignment

through guidance and mappings to make it is easier for organizations to use these frameworks together.

- NIST welcomes input on what they can provide to make the use of the Cybersecurity Framework 2.0 with the NICE Framework easier. They have been working closely with the NICE Framework team but welcome community engagement as well.
- NIST published a concept paper outlining their strategic direction for CSF 2.0. All comments on the paper have been made public. They want to ensure that the framework is usable by all organizations and addresses important topics like governance and supply chain risk management as well as cybersecurity assessment and measurement.
- On April 25, 2023, NIST released a discussion draft of the CSF 2.0 Core. The draft is meant to increase transparency but also to get input on the changes to the framework. They want to make sure that the feedback is incorporated into the full complete CSF 2.0 draft released for public comment this summer.
- The goal is to make sure that the framework remains flexible, outcome focused, sector and technology agnostic and can be used by all organizations regardless of sector. NIST wants to make sure that update process is increasing alignment with other resources including on cybersecurity workforce. The encourage members to participate in the updates, share feedback on the drafts and participate in upcoming workshops.
- Q&A:
  Q: Where does an organization start with using the framework if they must prioritize? What about the needs of small and medium businesses?
  A: The goal is that the framework is usable to all organizations regardless of size. They have increased engagement with small and medium sized businesses to see what level of guidance is needed and what are the gaps in terms of guidance to assist with implementation of the framework. The CSF website provides a multitude of resources to help. Some have been developed by NIST, by other federal agencies and various trade associations. The resources provide great starting places and additional detail on how to use the framework. In terms of where to start, with CSF version 1.1, it is a risk-based framework. The use of the framework will vary by organization. There are several sample profiles developed for specific sectors and for specific risk that can be a useful starting place. NIST believes the 'Identify' function of the framework is probably the most important function of all current five functions. Make sure the organization has a solid foundation of knowing what you already have and what your plan is to secure what you have is central to a cybersecurity program.
  Q: Is NIST working with the Center for Internet Security (CIS) on their eighteen controls?
  A: CIS participated in the second virtual workshop on CSF 2.0 and are involved in the in the update process.

VIII. Closing Remarks and Next Meeting Reminder

The next NICE Community Coordinating Council Meeting will be **May 24**, at 3:30 p.m. ET.