NICE Community Coordinating Council
Meeting Minutes
May 26, 2021 | 3:30-5:00 p.m. ET

I. Introduction and Ground Rules

NICE Program Manager Susana Barraza opened the meeting, reviewed the purpose and mission of the community, and explained the ground rules for the meeting. She encouraged everyone to participate e meeting via the Chat and reminded everyone that the space is not intended for any commercial use.

II. Opening Remarks

a. Industry Co-Chair: Jon Brickey, Senior Vice President at Mastercard

- A number of cyberattacks have been in the news lately, including the Colonial Pipeline attack, putting cybersecurity in the spotlight.
- The recently signed Executive Order on Improving the Nation’s Cybersecurity has generated a lot of discussions.
- With the COVID-19 vaccination roll-out proceeding, official business travel will be starting up in the next month or two.
- Jon presented a podcast related to the NICE Framework this week and gave a presentation on it last week. He has seen a lot of progress toward adoption of the Framework.

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

- There will be a presentation on the Executive Order on Improving the Nation’s Cybersecurity at the end of this meeting.
- NICE summer interns will likely be working virtually again this year. One of the things that shouldn’t change after the pandemic is virtual internships, not to say that in-person internships aren’t also important. Virtual internships offer flexibility and access for those who might not be able to travel.
- The FISSEA Summer Forum will take place June 17. Speakers will include Julie Haney and Karen Wetzel of NIST as well as the CISO at the Department of Health and Human Services. Additionally, there will be a keynote speech on cybersecurity human risk management and the importance of changing the focus away from viewing people as the weakest link to viewing them as a strategic asset.

III. Standing Items

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

MilGears
Presented by: Keith Boring, Director, Navy Credentialing Programs
URL: https://milgears.osd.mil/

The MilGears Cyber IT/Cybersecurity Workforce Tool allows job seekers to explore work roles and qualification requirements. It offers two ways to explore:

- View the Roles: Learn about specialty areas and work roles based on the NICE Framework. This tool provides role descriptions, examples of job titles, and the qualifications needed for basic, intermediate, and advanced positions.

- Customize Your Results: With this tool, users can input their own credentials and learn if they are fully, partially, or not qualified. It shows how to get to the next level in a career or how to move on to the next role. The customized results build a profile owned by the individual. It can be saved, and the outputs can be customized depending on who they will be sent to.

The tools are populated with data from the Navy's Credentialing Opportunities Online (COOL), but other data will be incorporated later this year. It also incorporates O*Net data, and it can be customized for non-defense related organizations.

b. Report Roundup - Learning from Good Ideas

ISACA Annual Cybersecurity Study
Presented by: Jon Brandt, Information Security Professional Practices Lead, ISACA
URL: https://www.isaca.org/go/state-of-cybersecurity-2021?utm_source=isaca&utm_medium=other&utm_campaign=research&utm_content=pr_research_state-of-cybersecurity-2021-part-1-press-release&cid=pr_2006993&Appeal=pr

Summary of Report Findings:

- Time to fill changed little since the last report.
- The number of respondents who believe that their cybersecurity team is appropriately staffed increased 3 percentage points.
- 68% of respondents whose organizations experienced more cyberattacks reported being somewhat or significantly understaffed.
- Retention remains difficult but improved slightly.
- Budgets are expected to increase.
- 50% of respondents generally do not believe that applicants are well qualified. College degree was at bottom of the list in terms of importance for qualifications.
- Hands-on cybersecurity experience remains a primary factor in qualification determination.

Unfilled roles:

- Unfilled roles increased slightly in 2021, but not to the levels of 2019, except for cybersecurity executives.

Skills Gap:

- Respondents largely view soft skills as the primary skills gap among cybersecurity professionals. Industry is talking about alternative ways of assessing people, such as asking for writing samples or asking candidates how they would approach particular situations.

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

New Curricula for National Cybersecurity Workforce Development Program
Presented by: Dr. Tirthankar Ghosh, Professor and Associate Director, Center for Cybersecurity, University of West Florida
URL: https://cyberskills2work.org/

The Cyberskills2work program provides free cybersecurity training and professional development, focused on recruiting and placing transitioning military, transitioning first responders, and veterans. Each of the programs offers a workforce pathway to work roles aligned to the NICE Framework. Courses award digital badges or certifications to participants who complete the programs.

New topics that will be mapped to the NICE Framework work roles include:
- Threat Intelligence and Hunting: Threat Analyst
- AI and ML for Cybersecurity: Data Analyst
- Malware Analysis: Cyber Defense Forensics Analyst
- Cyber Defense: Cyber Defense Analyst
- Digital Forensics: Cyber Defense Forensics Analyst

The goal moving forward is to create competencies mapped to the NICE Framework competencies, once they are incorporated.

d. Research Review

Cybersecurity Advocates: Discovering the Characteristics and Skills for an Emergent Role
Presented by: Julie Haney, NIST Visualization & Usability Group

Cybersecurity Advocate Work Role Characteristics:
- Promotes and raises awareness about cybersecurity jobs.
- Titles include security evangelist, security development champion, security consultant, among others.
- Must be able to address the technical and socio-technical aspects of the field.

Cybersecurity Advocate Qualities:
- Technical knowledge and skills – must understand threats well enough to establish credibility and trust with intended audience.
- Non-technical skills – interpersonal skills; context awareness; communications skills.
- Service Orientation – gravitate towards helping people; deep sense of the importance of the work.
- Discipline diversity – diverse educational backgrounds and work experiences; those from outside field can bring valuable skills; multidisciplinary teams.

Bolstering the workforce:
- Advancing the cybersecurity advocate role: Formalization of the work role; designing professional development training.
- Developing non-technical competencies: Becoming increasingly necessary for security professionals in general; professional development opportunities; incorporate into computing education curricula.
- Expanding the pipeline: Those with strong non-tech skills can thrive; framing cybersecurity as a service-oriented profession; hiring those with non-traditional background and skills.

IV. Working Group Updates

a. Promote Career Discovery
James "Jimmy" Baker, Cybersecurity Evangelist and Author or, Roland Varriale II, Cybersecurity Analyst, Argonne National Laboratory; or Monica Gomez, Cisco

- Added a third co-chair, Monica Gomez from Cisco
- Focused on addressing points made during an environmental scan and aggregating them into more strategic items that they can attach actions to.

b. Transform Learning Process
Dr. Aurelia T. Williams, Interim Vice Provost for Academic Administration, Norfolk State University; or Richard Spires, Instructor, Learning Tree

- At the June 9 meeting, the group will examine its final objective, which is about fostering proven learning methods to build and sustain a diverse cybersecurity workforce. At the last meeting they focused primarily on how to integrate multidisciplinary approaches.

c. Modernize Talent Management
Karen Jensen, Saaby Consulting; or Kevin Perry, Chief Cyber Training, DoD Cyber Crime Center/Cyber Training Academy; or Melissa Woo, Executive Vice President for Administration, Michigan State University

- Focused on exploring ways to measure success for the objectives that they have brainstormed strategies for.

V. Community of Interest Updates

a. Apprenticeships in Cybersecurity
Tony Bryan, Executive Director, CyberUp; or, Jennifer Oddo Executive Director, Strategic Workforce Education and Innovation, Youngstown State University

- Working on several projects, including a Comparative Analysis Report. Another project team is looking at the ROI of apprenticeships.
- They will be inviting a series of employers to speak at upcoming meetings to better understand the motivating factors for employers to build apprenticeship programs.

b. Cybersecurity Skills Competitions
Amelia Phillips, Highline College; or Brad Wolfenden, EmberSec

- Working on two ongoing projects ahead of CCAW: 1) scavenger hunt style competition; 2) panel discussion about ways people may find a career in cybersecurity
- US Cyber Games: US Cyber Games has an open application for participants and coaches. The program is also welcoming sponsors.

c. K12 Cybersecurity Education
Terrance Campbell, CCTE Cybersecurity Teacher, Shelby County Schools; or Laurin Buchanan, Secure Decisions

- The K12 Roadmap will be shared with the rest of the NICE community soon.
- The Open Doors one-pager is in final draft status.
- At the June meeting, there will be a presentation about how to prepare K12 students for internships.

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

- The NICE Framework Users Group started in January, and there are now more than 150 members. They are starting conversations about how the Framework can be used, what the challenges are, and more.

VI. Project Progress Reports

a. Cybersecurity Career Awareness Week
Presented by: Davina Pruitt-Mentle, NICE
URL: https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-awareness-week

- CCAW will be held the third week in October. Start brainstorming about how you can showcase careers in cybersecurity.

b. NICE Conference and Expo
Presented by: Randy Pestana, Florida International University
URL: https://niceconference.org/

- The NICE Conference and Expo will be held in person June 6-8, 2022, in Atlanta, Georgia. It will be held in June in subsequent years as well.
- Conference tracks will be announced this summer.
- Call for proposals will open September 7, 2021.
- FIU and the OAS will host an interim event September 14, 2021.
- The NICE Symposium, a half-day, hybrid event, will take place in November 2021.

c. NICE K12 Cybersecurity Education Conference
Presented by: Felicia Rateliff, Director of Operations & Programs, iKeepSafe
URL: https://www.k12cybersecurityconference.org/

- The NICE K12 Cybersecurity Education Conference will be held virtually December 6-7, 2021. They made the decision to hold a virtual event to ensure that all educators who may have difficulty with travel or budget can still attend.
- Call for Speaker Proposals is open through June 18 - proposal criteria are on the website.
- Cyber Signing Day: This sub-event during conference will feature 6 or 7 high school students who are participating in internships, apprenticeship, or training before May 2022. The event will feature a pre-recorded video. Interviews will take place beginning this summer through mid-October.
- They are looking for conference sponsors and exhibitors.

d. Centers of Academic Excellence (CAE) in Cybersecurity Community
Presented by: Tony Coulson or Amy Hysell, Cybersecurity Center, California State University, San Bernardino
URL: https://www.caecommunity.org/

e. Cyberseek

Presented by: Will Markow, Managing Director of Human Capital Management and Emerging Technologies, Burning Glass Technologies
URL: https://www.cyberseek.org

Recently Cyberseek went through a data refresh. Much of what is seen in the data is reflective of trends seen in the past.

- Over past 12 months, there were about 465,000 unique openings for cybersecurity jobs across the United States. This is slightly lower than what was seen in the past. It is likely a reflection of the pandemic and shifting hiring trends. They expect long-terms trend to show strong growth in jobs.

- There is evidence of a widespread talent shortage in cybersecurity. For example, over the past 12 months, there were about 145,000 job openings for information security analysts, but there is no way to fill them with people currently working in that field.
- The Career Pathway was updated to include another feeder role related to IT specialists.
- New enhancements planned for the coming months:
    - An additional enhancement to the Career Pathway: They will transition away from showing only roles to also providing a way to see skills and certifications that can be developed and the jobs they can qualify for based on those skills and certifications.
    - They plan to incorporate more information about training providers. If someone wants to prepare for a job in cybersecurity, they need to know where they can go to prepare for those roles. They will be able to look at training opportunities in their region. The data will be broken down by the type of program or training.

VII. Featured Topic

Executive Order on Improving the Nation's Cybersecurity
Presented by: Matt Scholl, Chief, Computer Software Division, NIST
URL: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity

- Matt testified at a May 25 hearing before the House Committee on Science, Space, and Technology on "SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains." A question was posed during the hearing about the need for an increased pipeline for the cybersecurity workforce. Currently, organizations are robbing qualified staff from each other and doing a disservice to the industry. The strategic issue is how to ensure a wider pipe of people entering the workforce and ensure they can find the necessary education.
- The Executive Order on Improving the Nation's Cybersecurity was drafted as a response to the SolarWinds attack, and it is focused on improving software security. It is 54 pages and includes eight sections. It is complex and encompasses a series of inter-dependencies - with various actions dependent on other actions. One section deals with expanding threat information sharing inside the federal government and between industry and the federal government. Another section looks at FedRamp, and another at maintaining and securing forensic information.
- Section 4, dealing with supply chain security, is where NIST is focused. It includes five main areas of responsibility:
    - ▪ Identify characteristics of critical software, which has not yet been defined. NIST has been given a 45-day deadline, and it is a tricky process.
    - ▪ Standards to be applied in a secure development lifecycle: What standards should be cited as best practice?
    - ▪ Issue best practices and guidance in securing a zzzz environment.
    - ▪ Software test tools: Look at the capabilities that good software testing tools should include.
    - ▪ Two pilot programs looking at product labels related to: 1) Internet of Things; and 2) secure software development practices. What are the deliverables that an organization should provide to give confidence they are following a secure development lifecycle?

- NIST will kick off the effort with a workshop on Enhancing Software Supply Chain Security. They have solicited position papers from industry in these different areas.
- The deliverables in this EO are fast and furious. The first deliverable was due today – DHS had to recommend what data should be maintained in a forensic lock file.

Q: How can people get engaged with this effort?

A: The initial deliverable is going to go very quickly. You can attend the workshop and provide your input. There will be ongoing iterations on critical software. The initial thought is to start with a discrete set of terms and definitions. Even though NIST has 45 days to come out with the initial criteria, that is just the start of a longer term process. Do not despair if you cannot get a meeting with NIST in the next 2 weeks. You can send a 2-page position paper up to the day of the workshop and it will be posted.

Q: What will be the impact on other NIST publications and guidance, such as the Secure Software Development guidance? Will that document be updated?

A: That document will be updated. They will use the SSD structure to ask people what they are doing in their lifecycle that achieves the outcomes in the guidance. They are struggling with how to apply how SDL applies to open source. How is your development environment being secured?

The November NICE symposium will look at issues related to supply chain security.

Q: The software supply chain section requires software vendors to follow a process and self-certify it. Is there concern that it will still be just a self-certifying checklist?

A: There is weight to self-certification. The liability is fully on the vendor rather than on a second or third party. Software is so dynamic and it can change multiple times in a day. A third party attester is probably not practical.

VIII. Closing Remarks Next Meeting Reminder

The next NICE Community Meeting will be June 23, 2021, at 3:30 p.m. ET