NICE Working Group

Meeting Minutes

Date: 10/26/2016 Time: 3:30 PM EST

SharePoint Page: https://nistgov.sharepoint.com/sites/NICEProgram/NICEWG

Strategic Plan for NICE: http://csrc.nist.gov/nice/about/strategicplan.html

I. Roll Call and Ground Rules

- Danielle Santos, NICE Program Manager, welcomed members to the meeting.
- During this meeting the Adobe Connect chat box feature should be utilized to provide feedback and ask questions.
- Danielle noted that participation in the NICE Working Group (NICEWG) is not intended for advertising and promotional purposes and to keep this in mind when participating and using the chat feature.

II. NICE Program Office Updates

- Rodney Petersen, Director of NICE, thanked members for joining.
- Members were reminded that the next NICEWG meeting has been moved to November 30th and that there will be no meeting in December.
- The K-12 conference, supported by NICE, was a great success. It is very exciting to see progress within the K-12 context as well as instructional content.
- Next week is the NICE conference in Kansas City, MO on November 1st and 2nd. The conference will include some special announcements such as:
    - The launch of the Jobs Heat Map through CompTIA and Burning Glass.
    - The publication of the NICE Cybersecurity Workforce Framework. Bill Newhouse will provide a preview toward the end of today's meeting.
    - The RAMPS announcements made several weeks ago will be unveiled during the conference. The awardees will discuss what they are doing and what their plans are. Those who were not selected should have received a notification email from Danielle Santos.
    - Coming soon is the annual launch of NICE. Now is the time to reflect, evaluate and provide feedback on the Working Group for improvements.

III. Opening Remarks

- President Kathi Hiyane-Brown, NICEWG Academic Co-Chair, is looking forward to meeting with the NICE staff, working group members and the general audience during the NICE conference. The conference will provide the opportunity to assess the work that the group has been doing, identify best practices and discuss future initiatives and where the group wants to go. Thank you for all of your continued work.
- Industry Co-Chair, Andre Thornton, also looks forward to the NICE Conference next week and especially the face-to-face engagement. Andre asked members, in preparation, to think about specific outcomes and activities to accomplish when meeting together. The group only has one opportunity to meet in person and it is important to pool everyone's energies toward the activities.

IV. Standing Items

a. **Event Engagement** – Presenter Alan Simpson provided a recap of the National K-12 Cybersecurity Education Conference.

   - The K-12 Conference took place a few weeks ago on October 1st and 2nd. The conference brought together a great group of people with a lot of diversity and a lot of great feedback was received. There were 189 people in attendance with 35% from K-12 and the rest primarily from higher education and government. 94% of the participants were extremely or highly satisfied. The sessions with the highest ratings were those that included students. Additional surveys will be sent out which will provide deeper feedback.
   - They are now looking toward the 2017 conference and thinking about ways to get more people involved. Next year, in looking for the best way to position the K-12 conference, they may want to piggy back off of another conference such as the High Impact Technology Exchange Conference in Salt Lake City, Utah, the CareerTech VISION conference in Nashville, TN, the National Career Pathways Network Conference in St. Louis, MO, or the Computer Science Teachers Association meeting in Baltimore, MD. Another opportunity would be to work next to a state cybersecurity conference. All feedback is welcome.
   - See slide presentation attached and find out more here: http://www.k12cybersecurityconference.org/

b. **Fun Facts** – Sara Hastings, Department of Labor, spoke about a recent report called "The State of Cybersecurity Professional Careers" as well as Cybersecurity Career Pathways.

- Sara works within the employment and training administration at the DOL and discussed a recent report about the state of cybersecurity professional careers as well as the work the federal government is doing in building and strengthening career pathway systems across the country.
- The report speaks to the challenges emerging and growing industries are facing. Most cybersecurity professionals struggle to define a career path. Advancement within a cybersecurity career is also a struggle and obtaining cybersecurity certifications are difficult. There are a number of industries and sectors facing similar kinds of problems. How do we train people and get the right partners, businesses and employers together to solve problems? How do we get credentialing partners together to credential for the right things?
- In 2011, the Department of State developed the original Career Pathways toolkit which outlined six key elements. However, in 2013, the Department of State and the Department of Health and Humans Services and Education realized it was beyond just education and labor and that technical assistance needed to be created. Thus, an interagency group on Career Pathways was created to develop guidance. The question of what do we mean and how do we define it still remained.
- In 2014, the Workforce Innovation and Opportunity Act was passed which laid out a clear definition allowing agencies to come together to define career paths. Additionally, in 2014, the Skills Working group was created. A sub-committee emerged from that group focused on career pathways. Recently, both groups were merged and a meeting was held last month bringing everyone together.
- In April 2016, a joint letter was created and posted by twelve federal agencies. It was a great accomplishment to get them together to think about career pathways.
- Recently there has been a new release of the career pathways toolkit guide which includes a workbook. The toolkit walks through six pathways with explanation. The toolkit is for state and local teams focused on workforce development, economic development and education. The workbooks walk through answering the hard questions. It speaks to specific questions that need to be answered to solve the problem of having the right people with the right skills, and how to have the right partners at the table. Feel free to reach out to Sara with any questions: Hastings.Sara@dol.gov

- The Career Pathways site is not a place to post internships. It is primarily to assist with workforce development at the state and local levels.
- The toolkit can be utilized by public and private sectors. There is a section specifically for employers that ask questions to guide a robust conversation on what one may need.
- Find out more about the career pathways portal sponsored by the U.S. Department of Labor, Employment and Training Administration here: https://careerpathways.workforcegps.org/
- To find out more about the report see attached presentation or follow the link below: http://c.ymcdn.com/sites/www.issa.org/resource/resmgr/press_releases/ESG-ISSA-Executive-Summary-S.pdf

c. **Report Roundup** - Marian Merritt, NICE Lead for Industry Engagement, spoke about "Cybersecurity Among Small Businesses in North America".

- Marian reported on a recent survey conducted by the Better Business Bureau with 1,500 BBB accredited businesses most of which are small businesses. 84% had fewer than 25 employees.
- The survey revealed that there is a high awareness of cybercrime and data breaches as well as awareness of impact on their businesses. The key take away is that the smaller the business the more likely they would turn to the BBB in the case of a data breach particularly because they don't have the resources to handle such an event themselves. Few small businesses have a dedicated in house IT person. 60% have some level of a readiness plan.
- The average small business's day to day concerns do not typically include cyber-attacks. They are focused on meeting payroll, retaining good staff, paying tax bills, the economic future, and keeping revenue and cash flowing. 70% of business owners believe it will happen to someone else. Even companies with over 250 employees thinks there is a 50/50 chance they will be affected. However, there is greater concern and awareness among larger companies.
- A big issue is a lack of awareness and training. Small businesses lack training resources, however the good news is that there is information and training available. The BBB provides the "5 Steps to Better Business Cybersecurity Training". The FTC developed the "Data Breach Response" guide. DHS has the C3 program. The

NCSA and DHS both have training materials available in addition to several others.

- In conclusion, the report recommends education outreach and training and a focus on the smaller companies who are most in need of education and training. The feeling is that certifications and credentials would be a good practice for businesses and their customers.
- See the attached presentation and find the full report here: http://www.bbb.org/stateofcybersecurity

d. **Strategy Stories** – Presenter Tina Ladabouche, NSA, spoke about the GenCyber program. This subject relates to the NICE Strategic Plan, Objective 2.3: Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school.

- The GenCyber program started due to the recognition of the need for qualified cybersecurity professionals in the workforce. The goal is to build a pipeline of individuals entering the workforce by reaching back to K-12 and teachers. The GenCyber program provides summer camps to students and teachers, mostly made up of middle and high school students, to assist students in understanding safe online behavior, increase diversity in careers, and improve teaching methods for delivering content. The camps are offered for students, teachers and a combination of both. Camps vary in size and duration from day camps to overnight lasting for one to several weeks. The camps are funded entirely by the NSA and NSF through grants.
- While the principles of cybersecurity are taught in the camps, the goal is more about hands on learning. There is only one piece of curriculum provided. Schools that host receive fundamental guidance but are free to be innovative in developing the curriculum. These camps also provide teachers the tools they need to take back to the classroom.
- In 2014 there were 8 camps, in 2015 there were 43 camps and in 2016 there were 120 camps held at 68 different institutions as well as in Puerto Rico and Washington, DC. Participation over the last cycle reached approximately 4,000 students and 1,000 teachers. The impact of the program has reached approximately another 50,000 students through the teachers who attended. The hope and intention is to have 200 camps by 2020 and have had at least one camp in every state.

- The camp location does not have to be at a college. They can be at a non-profit with an education component. However, funding must be at no cost to any participant.
- The GenCyber website outlines information on the proposal requirements. Proposal review will begin in December and decisions on the camps will be made in January. See slide presentation attached and find out more here: https://www.gen-cyber.com/

e. **Metric Moment** – Ellen Klicka, Raytheon Company, discussed the Cybersecurity Talent Gap.

- Ellen discussed a survey, which is in its fourth year, by the Raytheon Company and the National Cyber Security Alliance (NCSA). The survey focused on the career interests and preparedness of millennials ages 18-26 in order to provide insight into today's cybersecurity workforce shortage.
- The results conclude young adults do care about and are interested in cyber. They see the need in politics as well as in their daily lives and careers but need more opportunities, exposure and guidance. Young adults could be a significant part of the solution.
- Awareness and media coverage of cyber-attacks is growing worldwide. Cyber awareness campaigns have been effective, however, the gender gap continues to widen.
- Enrichment activities and career exploration incentive programs in cyber are becoming increasingly available to millennials worldwide and especially in the Middle East. With more programs available there are more young adults taking advantage of the opportunities. Still, there remains a significant gender gap.
- There is a positive trend of young adults receiving exposure to lessons in cyber safety in schools and the numbers continue to improve.
- Parents play a large role in guiding their child's job path but their influence does not match their child's ability to guide them toward a career in cyber. This speaks to the need for targeting parents in efforts to close the talent gap.
- Finally, the survey found that approximately 53% of millennials are influenced by the candidate's positions on cybersecurity and 50% feel that cybersecurity has not been a big enough part of the discussion leading up to the presidential election.

- See attached presentation and find out more here: http://www.raytheoncyber.com/news/feature/2016_cyber_survey.html

V. Subgroup Updates

- **K-12**
  - Davina Pruitt-Mentle informed members the K-12 subgroup have been working on their deliverables such as the national K-12 implementation plan. The implementation plan will be shared at the NICE conference. There are a number of one-pagers in the works but they may not be ready in time for the conference next week.
- **Collegiate**
  - Barbara Endicott-Poposky reported that the group has several new members. Barbara will be rotating off as co-chair in December but hopes to continue to play an active role.
  - The Collegiate subgroup is looking at areas for consideration and focus such as entry level jobs, jobs fairs, student associations, minorities in education, pathways and professional development of educators.
- **Competitions**
  - Dan Manson reported that the competitions one-pager was released and made available at the K-12 conference. The Competitions white paper is in its final stages and will be released at the NICE conference. The paper includes input from twenty-five thought leaders in cybersecurity. Dan hopes everyone will take the time to read it and provide feedback. The paper notes that there is a shortage of cybersecurity professionals but the level of incoming talent needs to rise. Cyber competitions can help increase the talent.
  - Recently there was a capture the flag competition in Washington DC which occurred at the same time as CyberMaryland. The competition had great speakers and both the beginning and the end of the competition were live-streamed. The competition is also available on YouTube. Running a competition for broadcasting is a great opportunity.
- **Training and Certifications**
  - Linda Montgomery informed members that the Training and Certifications subgroup has been very busy. The Cyber Range project group has put out a one-pager which indicated the what,

why, who and where of Cyber Ranges. It is evident from the graphic (see attachment) that we are identifying those cyber ranges to be in compliance with the National Workforce Strategy.

- A new project group working to map credentials to work roles and KSAs has been very busy. Linda recognized Chris Kelsall, Ken Slaught and Doug Rausch for their invaluable work. The working document lays out the work roles and looks at categories linearly while also looking at vendor credentials. These are then mapped to entry level, intermediate and advanced levels. The document helps to identify where the gaps are occurring as well as set standards. Additionally, they are looking at the level of proficiency apart from credentialing.
- See attached presentation

- **Workforce Management**
  - Maurice Uenema provided updates on the work of the Workforce Management subgroup.
  - Literature Project Team update: The Workforce Management subgroup recently created a literature review project team after the work of the charter team came to a close. The intent of the group is to assess existing works related to managing the human elements of cybersecurity risks. The hope is that this work will guide the subgroups efforts on the enterprise side of things. If anyone is interested please reach out to Maurice Uenema (muenuma@tripwire.com) or Kristin Judge (kristin@staysafeonline.org).
  - KSA Project Team Update: The Role/KSAs project team, led by Frank Cicio and Leo Van Duyn, efforts actively continue. They are adapting roles and KSAs to make them more industry specific. They have also identified new roles specific to the financial industry.
  - Human Factors Project Team Update: The group has developed a draft construct or model for looking at the entire Enterprise Workforce as it relates to cybersecurity risk with tight linkage back to the NIST framework. The group will be reviewing this during the next subgroup meeting.

VI. Project Progress Reports

- **NICE Annual Conference**
  - The upcoming conference has an app which can be downloaded on your phone. The app is: WHOVA. Conference attendees can

use this app to start setting up their specific agendas. The app is also a good place to receive updates throughout the conference.
    - There will be a NICE Working Group session on November 1st at 10: 15 AM. The five subgroups will present on their focus and what they have been working on.
    - Additionally, the NICE projects: NICE Challenge, CAE Community and Jobs Heat Map will all have booths at the conference which everyone should feel free to stop by.
    - Additional information can be found through the following link: https://www.fbcinc.com/e/nice/

VII. New Business – Bill Newhouse, Deputy Director, NICE discussed the Draft NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework.

- The updated NIST special publication (draft) 880-181, will be open for public comments on Wednesday, November 2nd. There are about seventeen pages of narrative describing the function, applicability and components. The tables include what has been seen in previous versions but will have finer details. It describes the broad terms of cybersecurity work. There are still seven high level categories and over 50 work roles where each position may have 3-5 work roles. Organizations may pick and choose what is relevant to their workforce.
- A common lexicon identifies standards to make it easier for training providers. This can answer questions such as which certification will matter to me? The hope is that this publication leads to a capable and ready workforce.
- There will be a press release sometime next week to build energy and deliver comments.
- For more information see attached presentation and click here for more information: http://csrc.nist.gov/nice/framework/

VIII. Member Questions

There were no additional questions from members.

IX. Summary of Action Items – meeting notes, presentation, and URLS will be sent to all members. Please remember to send in events you know about or are planning to attend.

X. Next Meeting Reminder -The December and November meetings will be combined into one due to the holidays. The combined meeting will take place on November 30th.