**NICE Working Group**

**Meeting Minutes**

**Date: 8/23/2017 Time: 3:30 PM EST**

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

1. **Introduction and Ground Rules** 
   * Danielle Santos, NICE Program Manager, welcomed members to the meeting. The NICE Working Group is setup to provide a mechanism for collaboration between academia, government and industry and to discuss strategies and actions to aide in workforce development.
   * 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.
2. **NICE Program Office Updates** 
   * Bill Newhouse, Deputy Director of the National Initiative for Cybersecurity Education (NICE), thanked everyone for joining and encouraged participation and engagement during the meeting.
3. **Opening Remarks**
   * Academic Co-Chair, President Kathi Hiyane-Brown, welcomed members to the call. President Kathi noted that the NICE staff and working groups have been very busy this summer and thanked everyone for their hard work. She is very excited to start off the new year as most universities are coming off of summer break.
   * Industry Co-Chair, Andre Thornton, welcomed members to the call and echoed President Kathi’s sentiment and excitement in starting a new fiscal year for both schools and the government.
4. **Standing Items** 
   * **Fun Facts** – Laura Bate presented on New America’s article on Attracting More Cybersecurity Talent.
     1. New America is a non-profit and think tank based in Washington, D.C.
     2. Laura noted that garnering a holistic picture of federal government hiring in cybersecurity, despite the variety in sectors from which their data is derived, is difficult given the lack of data.
     3. A most common reason for limitations in hiring is funding. Coming up with benefits packages to match those of the private sector employers is not easy.
     4. The federal government does not have a monopoly on mission driven incentives. However, the government does offer unique training capabilities. Interesting and ongoing training can attract new talent and keep it.
     5. New America has been looking at apprenticeships in cybersecurity. A few issues they have heard about apprenticeships include difficulty around registration as well as changes to program duration and method. The minimum length for an apprenticeship has been dropped to one year. Also, new methods of apprenticeships have been introduced. There are now competency based and hybrid models.
     6. Some of the benefits for apprenticeships include structural flexibility. Coming up with a one-size fits all program is difficult so flexibility of apprenticeship programs is helpful. There are many ways to set up a program to tailor it to ones needs. Additionally, there are the tax and tuition benefits that come along with an apprenticeship. The educational components are often tied to associates degrees.
     7. The room for growth in cybersecurity includes apprenticeships in four-year settings that would proceed through a bachelor program. There is great importance in ensuring that credits are transferable to students.
     8. There is also an opportunity for stakeholder collaboration. Programs should not start from scratch. Apprenticeship sponsors could and should be sharing their resources.
     9. Finally, there is always a need for more data. Of particular interest is as student’s graduate from these programs, where do they end up? New America is looking at ways to measure outcomes as students graduate.
     10. A member inquired about the minimum academic qualifications and credentials for the apprenticeship programs. Laura responded that it depends on the case as some programs are very flexible.
     11. See the attached presentation for more information and find out more here: <https://federalnewsradio.com/training-cyber-workforce/2017/08/one-easy-thing-your-agency-can-do-to-attract-more-cybersecurity-talent/>
   * **Report Roundup** – Isabel Cardenas reported on ‘Investing to Improve the Cybersecurity Talent Deficit’.
     1. Isabel works with Business-Higher Education Forum (BHEF) and is very excited to share the work they have recently completed in cybersecurity recommendations. BHEF supports collaboration between business and higher education. They work with their stakeholders to build regional talent echo systems.
     2. Over the last year BHEF have put out three different reports. The reports can be found through the following link: [www.bhef.com/publications](http://www.bhef.com/publications). To create their recommendations report, information was pulled from the three reports.
     3. There are three different areas for their recommendations.
        1. Collaboration: what are the specific ways employers can build up the pipeline and how can higher education better prepare their students for cybersecurity careers and pathways.
        2. Building a skills framework that both business and higher education can use.
        3. Building consensus on security standards and learning from other organizations about security threats.
     4. BHEF is interested in ways to attract students into cybersecurity and become part of the workforce. The number of women is increasing and the population overall is more diverse than in the past.
     5. Academic institutions can partner with employers to create relationships to hire students.
     6. See the attached presentation for more information and find out more here: <http://www.bhef.com/sites/default/files/bhef_2017_invest_to_improve.pdf>
   * **Strategy Stories** –Tim Blute reported on the ‘States Pledge to Meet the Cyber Threat’. This topic supports the NICE Goal 1: Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers.
     1. Tim is with the National Governors Association who just completed a year-long cybersecurity initiative. The goal of the initiative was to raise awareness of cybersecurity threats and to implement best practices. Their work focused on two specific areas: workforce and economic development.
     2. The culmination of their work has allowed governors to sign up and acknowledge the importance of cybersecurity at the state level. By signing, they acknowledged they will work to move forward on cybersecurity issues. 39 governors have signed up thus far.
     3. The association can and will assist these governors through best practices. They will keep track of what states and governors are doing in this space.
     4. See attached presentation and find out more here: <https://www.nga.org/cms/news/2017/states-pledge-to-meet-the-cyber-threat>
   * **Metric Moment** – Rebecca Dalton presented on CyberPatriot Impact Metrics
     1. The Air Force Association’s CyberPatriot program was created to attract interest in STEM (Science, Technology, Engineering and Math) careers in cybersecurity.
     2. It is important to know if their program is working and for their stakeholders to know their participation is worth it. A survey was created and sent to the participants. The majority of the 2,871 responses were male with 23% female.
     3. The survey inquired of students about their post high school plans. 88% of those that responded said they plan to pursue a 4-year degree in cybersecurity.
     4. Questions can be emailed to: [Info@uscyberpatriot.org](mailto:Info@uscyberpatriot.org).
     5. See attached presentation and find out more here: <https://www.uscyberpatriot.org/about/impact>
   * **Event Engagement** – Princess Young spoke to the National Cybersecurity Awareness Month Activities.
     1. The National Cybersecurity Awareness Month (NCSAM) takes place in October and is run by the Cybersecurity Education and Awareness (CE&A) Branch of the Department of Homeland Security. This will be the 14th year celebrating the month.
     2. DHS leads an annual, nation-wide effort with the National Cyber Security Alliance to raise cyber awareness. It is a collaborative effort between both government and industry to ensure Americans have the resources they need to stay safer and more secure online, and increase the country’s resiliency in case of a cyber incident.
     3. Starting in 2004, NCSAM has been formally recognized by the president, congress: federal, state, and local governments, and leaders form industry and academia.
     4. CE&A co-manages and co-leads the program. Each week has a different theme during the month of October (see slides for theme descriptions). They decided to break the month out into digestible themes to plan around.
     5. If you want to participate it is important that you start planning as early as possible. To have the best speakers and materials it is best to plan ahead of time.
     6. The White House releases an annual Presidential Proclamation in late September/early October on National Cybersecurity Awareness Month. The White House also encourages federal government agencies to participate.
     7. The DHS CE&A will work with anyone to ensure their awareness month is a success. Resources for stakeholders to plan events and initiatives will be provided. Any reports shared with them are housed.
     8. They provide NCSAM Partner Packets which include a planning checklist, ideas for activities, turn-key content and sample articles for each of the weekly themes. They will ensure that NICE has this information to share with its members as well.
     9. Think about your goals and how they tie to some of the weekly themes if you wish to participate. How can you use this as a pivotal launching pad for any of your initiatives for this fiscal year?
     10. The official NCSAM hashtag is: #CyberAware
     11. Email [stopthinkconnect@dhs.gov](mailto:stopthinkconnect@dhs.gov) for more information on how to view online events.
     12. Feel free to email Princess Young for additional information at: [princess.young@hq.dhs.gov](mailto:princess.young@hq.dhs.gov)
     13. See attached presentation and find out more here: <https://www.dhs.gov/national-cyber-security-awareness-month>
5. **Subgroup Updates** 
   * **K-12** - Carlos Garcia, co-chair, provided the K-12 update.
     1. Carlos reported that the K-12 Conference is moving forward nicely and Davina has submitted formal RFI ideas.
     2. The group is about to put together a project directory and are now working out the bugs.
     3. They are looking to add CTE education programs to their existing template on a K-12 Project directory.
     4. The subgroup is working very hard to make their first Cybersecurity Career Awareness week a success. The week is planned for November 13th - 18th. The website will go live next week.
   * **Collegiate** –Heather Monthie, co-chair, provided the Collegiate update.
     1. The Collegiate sub-group has two main project teams.
     2. The first project team is looking at different academic pathways for cybersecurity careers. The group has been at a standstill but now has a new project lead. The Collegiate co-chairs will be working with the new lead to get that project caught up.
     3. The second team is looking at different tools and technologies to demonstrate student’s skill sets. They are collecting information on tools and technologies that are already available. They are also developing a framework for student portfolios. The group is also planning to create a white paper as well as present at the NICE Conference in November.
     4. Heather also noted that the Collegiate subgroup has grown from 28 members at its start to 91 which indicates a substantial growth. However, the representation is largely academic so they would like to see more industry and government involvement.
     5. The next Collegiate subgroup meeting is on September 12th.
   * **Competitions** –Jessica Gulick, co-chair, provided the Competitions update.
     1. The next Competitions subgroup meeting is this Friday, August 25th at 3:30pm.
     2. The subgroup has restructured their meetings to now include a speaker. Last month they heard from two MITRE students giving an update on their internships. This month they will hear from Karen Evans and Katie Hansen on CyberCompex.
     3. The group is very focused on 2018 and, in part, transitioning to new leadership.
     4. They are looking at more speaking opportunities and planning a leadership summit.
   * **Training and Certifications** – no update
   * **Workforce Management**- Kristin Judge, co-chair, provided the Workforce Management update.
     1. This subgroup are continuing to make progress in building the workforce management guidebook. They have had some slippage in their timeline but continue to make headway in developing the content. They will be pulling all of the information into a first rough draft. The content will be ready for the broader NICE Working Group review by October. The co-chairs continue to request your involvement and support.
     2. Contact the co-chairs here: [muenuma@tripwire.com](mailto:muenuma@tripwire.com), [kristin@staysafeonline.org](mailto:kristin@staysafeonline.org)
6. **Project Progress Reports - Amber Lindsay**
   * **NICE K-12 Cybersecurity Education Conference** 
     1. The conference will be held December 4-5 in Nashville, TN at the Omni Hotel.
     2. There are several confirmed keynote speakers to include: Chrissy Haslam (First Lady of Tennessee), Diane Miller of Northrop Grumman and Kim Ford.
     3. There are 40 plus speakers lined up this year.
     4. Interactive hands on workshops have been scheduled as well as question and answer lightning rounds. They are working with the American School Counselor Association to put together a counselor panel and are working on a student panel as well.
     5. The tentative agenda is currently online. The final agenda will be announced next week and will be available for download.
     6. There is now early bird admission as well.
     7. Find out more here: <https://www.k12cybersecurityconference.org/>
   * **NICE Annual Conference - Danielle Santos**
     1. An announcement went out this morning that the NICE Conference agenda is now available on the conference website.
     2. The agenda tab is up so anyone can see all of the different tracks. The speaker bios are available as well.
     3. The details on the pre-conference seminars can also be found on the website. The seminar registration is offered with the registration for the main conference. The three seminars include:
        1. Critical Success Factors for a Cybersecurity Apprenticeship Program
        2. How to Build Robust Internship Programs Between Employers and Academic Institutions
        3. Application and Uses of the NICE Cybersecurity Workforce Framework
     4. Find out more here: <https://www.fbcinc.com/e/nice/default.aspx>
   * **NICE Challenge Project – James Ashley, Project Manager**
     1. The project has reached 65 challenges which are currently available on the portal.
     2. The NICE Challenge Project now has over 150 officially registered educational institutions in the U.S. There are now over 200 curators in the portal this month as well.
     3. Most releases this month have been updates to the portal itself. There are four new challenges available.
     4. The team has been hard at work moving features from inside the environment pods to outside in the web portal.
     5. They are very close to finalizing the 1.0 release with active marketing going on now.
     6. Find out more here: [https://www.nice-challenge.com](https://www.nice-challenge.com/).
   * NICE Jobs Heat Map – Randi Parker, CompTia, provided an update
     1. GIAC data was recently added to improve comprehensiveness of the certification reflected in the tool.
     2. A new pdf about ‘Cyberseek’ is now available to download which can be shared to raise awareness about the tool.
     3. A complete refresh of the demand and employment data in Cyberseek with data from Q2 2016 through Q1 2017 was performed.
     4. Some statistics from the data refresh include:
        1. From Q2 2016 through Q1 2017, there were nearly 300,000 openings for cybersecurity-related roles in the U.S. There were also nearly 747,000 employed cybersecurity-related workers, meaning there were 2.5 employed workers for every opening. While this is an improvement over the previous supply/demand ratio of 2.2, it is still far below the job market average of 5.6 employed workers for every opening. Said another way, if the supply of cybersecurity workers relative to demand were to be in-line with the market average, it would have to more than double overnight.
        2. For cybersecurity’s most important job – Information Security Analysts – there were 112,000 openings but only 96,870 workers currently employed in those positions. This reflects an annual talent shortfall of over 15,000 workers for cybersecurity’s largest job.
        3. The NICE category with the greatest demand was Operate and Maintain, with 194,000 openings. This reflects the pervasiveness of security demand outside of traditional security-related roles into the broader IT landscape.
7. **New Business**

* Laurin Buchanan spoke about the Competitions Survey Instrument
  + 1. Laurin is a member of the Competitions subgroup. The subgroup has put together a survey to gather feedback about people’s experiences and awareness about cybersecurity competitions.
    2. The survey is anonymous. The Competitions subgroup requests that people share the survey link through any means. Laurin will put together a brief description of the survey if anyone needs it.
    3. Some of the respondents thus far include mentors and coaches. Others are identified as professional workforce.
    4. The survey will remain valid and available for the foreseeable future. The information will be used to help guide the subgroup.
    5. The survey can be found through the following link: <https://www.surveymonkey.com/r/YPXPX8V>
  + Bill Newhouse spoke to the NICE Framework
    1. Bill Newhouse is the Deputy Director of NICE and one of four authors of the NICE Workforce Framework.
    2. Cybersecurity work was broken down into seven categories. The categories were then broken down into 33 specialty areas: distinct areas of cybersecurity work. Finally, the specialty areas were then further broken down into 52 different work roles.
    3. When looking at tasks, the framework shows affiliated work roles. The work roles are the most specific things in the document with more than several hundred tasks, knowledge and ability statements.
    4. Flexibility was a main goal for the authors. This is a super set of things that are broken down into work roles. You don’t have to have them all but rather have the ability to pick and choose. The framework allows employers to communicate requirements for their positions and needs. Employees can use the lexicon in this framework to communicate their needs and improve their training. Training and certification providers have already started mapping their courses to the framework.
    5. The document has been developed over several years. The Special Publication allowed them to take on comments through NIST. There were nearly 1,000 comments in total. The final product is their best effort to put together a cybersecurity dictionary.
    6. A one-pager has been created around the NICE Framework.
    7. A revisions page has also been created with a process outlining submittal of revisions requests. Additionally, a change log was created to keep note of why some change requests might be denied.
    8. An email box on the framework page will eventually be added.
    9. Additional information can be found through the following link: <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

1. **Summary of Action Items** – Minutes and presentation materials will be sent to all members.
   * The Collegiate subgroup is seeking industry members to join the group: [nicewg.collegiate@nist.gov](mailto:nicewg.collegiate@nist.gov)
   * Please feel free to share out the Competitions Survey link: <https://www.surveymonkey.com/r/YPXPX8V>
2. **Next Meeting Reminder** – The next NICEWG meeting is scheduled for September 27, 2017