**NICE Working Group**

**Meeting Minutes**

**Date: 8/22/2018 Time: 3:30 PM EST**

**Click** [**here**](https://www.nist.gov/itl/applied-cybersecurity/nice) **to view the NICE Website**

**SharePoint:** [https://nistgov.sharepoint.com/sites/NICEProgram/NICEWG](https://nistgov.sharepoint.com/sites/NICEProgram/NICEWG/Pages/home.aspx)

# Introduction and Ground Rules

* Danielle Santos, NICE Program Manager, welcomed participants to the meeting. The NICE Working Group (NICEWG) is setup to provide a mechanism for collaboration between academia, government and industry and to discuss strategies and actions to aid in workforce development.
* During this meeting the Adobe Connect chat box feature should be utilized to provide feedback and ask questions.
* The NICEWG is not intended for advertising and promotional purposes and to keep this in mind when participating and using the chat feature. She urged all participants to collaborate and share information while working on projects.

# NICE Program Office Updates

## Marian Merritt, NICE Lead for Industry Engagement, provided the update.

## There is newly launched resource material that everyone should be aware of. It is a new series of instructional webinars covering a variety of cybersecurity education and workforce development topics.

## The membership requested information on these areas and the NICE summer interns helped to put it together. Some have additional materials available for download. The currently uploaded topics are: Resume Writing, Interviewing Techniques, and NICE Cybersecurity Workforce Framework 101.

## The tutorials can be viewed [here](https://www.nist.gov/nice-tutorials).

# Opening Remarks

## Academic Co-chair President Kathi Hiyane-Brown provided the remarks.

## The academic world is preparing for the fall season and starting a new school year. Work on preparing new grants, activities, and hiring new faculty has been ongoing. It has been difficult for higher education institutions to hire qualified instructors.

## One of the best methods has been to seek instructors among graduates from the institution. Students returning to their alma mater to teach has been a great way to give back and we applaud those students, and instructors to persuade them to return.

# Standing Items

## **Report Roundup**

### Gary Davis, Senior Director in Consumer Business, McAfee presented on, "Winning the Game", gaming in the cybersecurity workforce.

1. McAfee commissioned a survey to try to understand what tools and strategies might be needed to combat threats, and what are the capabilities and characteristics of organizations that appear to be better equipped to deal with current threats. The survey was sent to organizations with 500 or more employees in the U.S, U.K., Germany, France, Singapore, Australia, and Japan.
2. The goal was both to understand key challenges facing IT security organizations related to threats, technology investment, and skills; as well as to attempt to identify strategies and techniques to fight back.
3. Use of gamification was a key area to boost effectiveness of defense against threats.
4. They began looking at gamer proximity to cybercrime. A survey was developed to look at ways to use automation for cybersecurity paths and introducing gamification to increase understanding for IT staff.
5. Most people interviewed (about 1,000 IT managers) believe gamers possess the skills that are needed in cybersecurity.
6. Hiring managers tend to look for people who examine the edges, looking for how to get through something faster.
   * One popular technique in player vs player gaming is booting, that is, launching an attack to get an opponent offline.
   * There are challenges in working with gamers. Some struggle to incorporate well into corporate life.
7. We continue looking at how we can make the linkage into the gaming world and how to bring more of them into cybersecurity positions.
8. See presentation attached and find out more [here](http://www.information-age.com/uk-education-system-exacerbating-cyber-skills-gap-123468601/) .

## **Strategy Stories**

### Aric Perminter, International Consortium of Minority Cybersecurity Professionals (ICMCP) presented on "International Consortium of Minority Cybersecurity Professionals".

1. [ICMCP](https://icmcp.org/careers) is a non-profit that works with partners like NICE to work toward adoption of cybersecurity awareness and education. The goal is to give students the opportunity to do the job they want to do when they get out of college, as well as to bridge the divide facing women and minorities in the cybersecurity field.
2. ICMCP works through four programs:
   1. Scholarships through the [Cybersecurity Scholarships Program](https://icmcp.org/scholarship_academic) .
   2. Mentor- protégé relationships through the [Mutual Match Protégé Program](https://icmcp.org/programs/mutual-match-mentor-protege/) .
   3. [Center for Professional Development](https://icmcp.org/careers) through maintaining relationships with industry and business leaders to facilitate internship, job readiness, and job placement.
   4. Cybersecurity Workforce Development through talent acquisition and recruitment services, and Educational Security Operations Centers (eSOC).
3. eSOCs are cyber ranges that can be stood up at universities so that students can simulate the job they will be performing in their career after graduation.
   1. Cyber range use makes sure the book smarts are being matched to hands-on experience. Participants receive hands on training with all things relating to cyber operations. They help teach how to protect their company’s environments.
   2. How is training organized? They don't want students to train in one role only. Thinking with the end state in mind helps prepare and increase success along the career path.
   3. Preparing individuals to have the KSAs that align to the experience and skills needed. They are also helping to write job descriptions that are generic. Hope to have parties in the process speaking the same language for all stakeholders.
   4. They are also helping to write job descriptions that are generic with the hope to have all stakeholder speaking the same language.
   5. See presentation attached and find out more [here](https://icmcp.org/) .

## **Metric Moment**

* Laura Hatzes, NICE Associate, presented on the NICE Website metrics.

1. Two years ago, the program office embarked on an initiative to migrate the content from the existing NICE website to a new platform. This new platform improves the visual layout of the pages and provides easier navigation. The new NICE website was officially launched on May 1st, 2017.
2. Google analytics is the web analytic service that tracks the website activities. A metric report is developed every six weeks and contains four high level sections. These sections include reporting on behavior such as pageviews, bounce rates, and average time spent on the page. The report contains information on where people are coming from and what types of devices are used. Finally, the report includes event behavior such as file downloads. It is important to track the NICE resources such as the NICE workforce framework supporting materials and the NICE one pagers.
3. In addition to reporting data, observations that might be notable for that timeframe are highlighted upfront. Typically, this data consists of general numbers such as overall pageviews and unique pageviews and average time spent on all pages. Information that may be unique to that timeframe is added. As an example, the eNewsletter page is developed on a quarterly basis so it’s important to highlight performance for this page and show comparisons to previous eNewsletter pages.
4. The program office is always interested in feedback and suggestions from the working group. The NICE website is continuously refreshed, and new pages are added with information and resources that are pertinent to NICE initiatives. We want to be sure the website is correctly promoting the work of the program office, the working group and the subgroups. The hope is that the website is well organized and most importantly that the audience finds the information they are looking for.
5. Suggestions and feedback can be sent to [nicesupport@nist.gov](mailto:nicesupt@nist.gov)
6. See attached presentation and find out more [here](https://www.nist.gov/itl/applied-cybersecurity/nice) .

# Subgroup Updates

## **Apprenticeship**

* Marian Merritt provided the update.

1. This subgroup created a subproject to perform a landscape survey. This project team is looking at existing cybersecurity apprenticeship programs, programs in development, and programs registered with DOL or the state.
2. Carolyn Renick, DOL, developed a spreadsheet listing known apprenticeship programs. Jennifer Carlson and others have added data to the spreadsheet. The project team has discussed data elements to capture.
3. The full Apprenticeship subgroup meets the fourth Friday every month at 11 a.m., Eastern Time.
4. Visit the Apprenticeship website [here](https://www.nist.gov/itl/applied-cybersecurity/nice/apprenticeship-sub-working-group) .

## **Collegiate**

* Stephen Miller, co-chair, provided the update.

1. The academic pathways project has been looking at developing various pathways that align to work roles.
2. The tools, techniques, and skills project team are working to finish a one pager by the end of September.
3. The subgroup is putting together a new project team to discuss the value of higher education.
4. The next subgroup meeting is 9/11.
5. Visit the Collegiate website [here](https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/collegiate-sub-working-group) .

## **Competitions**

* Laurin Buchanan, co-chair, provided the update.

1. Podcasts on various competitions topics are being developed and can be found [here](https://www.youtube.com/cyberfed). Subgroup members will try to post one per week. Working group members are encouraged to listen to the podcasts and pass the word on the podcasts to anyone interested. Subgroup members are open to suggestions for future topics.
2. This subgroup is using #cybercompetition on social media. They are looking to leverage the podcasts and a variety of cybersecurity competition related information.
3. Laurin mentioned wanting to meet someone from DOL, or anyone with experience in cyber competitions.
4. For a potential future project, the subgroup is discussing competency metrics. The idea is to map competencies in competitions to the [NICE framework](https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework).
5. The subgroup meets the fourth Thursday each month at 3:30 p.m. Eastern Time. The next meeting is September 27.
6. Visit the Competitions website [here](https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/competitions-sub-working-group).

## **K12**

* Patrick Schultz, co-chair, provided the update.

1. The K12 subgroup did not meet in August. Many members are preparing for the upcoming school year.
2. The next meeting is scheduled for 9/12. There will be a presentation for career technical student organizations targeting 6-12 graders.
3. Visit the K12 website [here](https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/k-12-sub-working-group) .

## **Training and Certifications** – No update.

## **Workforce Management**

* Marian Merritt, NICE Lead for Industry Engagement, provided the update.

## A good amount of feedback has been received on the “Cybersecurity is Everyone’s Job Guidebook”. The draft guidebook can be downloaded [here](https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/workforce-management-sub-working-group/workforce).

## Consolidating responses and editing will be ongoing. The goal is to publish in September. The guidebook will be in pdf format and consists of seven subcomponents relating to business functions.

## The National Cyber Security Alliance will be promoting the guidebook on social media during week 3 of the National Cyber Security Awareness Month.

## The next subgroup meeting is 9/20.

## Visit the Workforce Management website [here](https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/workforce-management-sub-working-group) .

# Project Progress Reports

## **National Cybersecurity Career Awareness Week (NCCAW)**

* Danielle Santos, NICE Program Manager, provided the update.

## Planning for NCCAW has been ongoing. The K12 subgroup has played a major role in planning.

## It's important to include recent graduates, veterans, and other IT professionals to raise awareness.

## NCCAW planning will be part of the regular updates from now until the conference takes place November 13-18, 2018.

## The goal to refresh the website in the next two weeks with new content and resources.

## Visit the NCCAW site [here](https://www.nist.gov/itl/applied-cybersecurity/nice/events/national-cybersecurity-career-awareness-week).

## **NICE K12 Cybersecurity Education Conference**

* Danielle Santos, NICE Program Manager, provided the update.

## The conference is scheduled for December 3-4, 2018 in San Antonio, TX.

## Registration is now open. There are three pre-conference workshops: hacking resources, classroom cyber ranges, and resources for teachers.

## Visit the K12 [conference registration](https://www.k12cybersecurityconference.org/registration/) site to secure hotel rooms at the K12 conference room rate. Those rooms are filling up fast.

## Find out more [here](https://www.k12cybersecurityconference.org/).

## **NICE Annual Conference**

* Randy Pestana, Florida International University, provided the update.

## The conference is being held November 6-7, 2018 in Miami, FL. Early bird registration is open until the end of August.

## This year's early bird fees are lower than last year. Fees will increase after the end of August.

## A preliminary agenda will be available in the next few weeks. Please email [info@niceconference.org](mailto:info@niceconference.org) with questions. Hotel rooms are available [here](https://niceconference.org/registration).

## Find out more [here](https://niceconference.org/) .

## **NICE Challenge Project**

* James Ashley California State University, San Bernardino, provided the update.

## The summer development window is ending.

## The project has had 250 higher education institutions register with approximately 375 curators (educational faculty and staff).

## They are looking forward to the upcoming usage data and anticipate an increase in activity once the academic year starts. They will be at over a hundred thousand virtual machines.

## Two thousand workspaces have been deployed. The user base continues to grow. The project is expecting to release new challenges in the next few months, possibly 10-15 new challenges by the end of the year. Visit [here](https://nice-challenge.com/) for more information.

# New Business

## **Cybersecurity Presidential Management Fellow**

## Rob Timmons, OPM, presented on the Cybersecurity Presidential Management Fellow program.

## Rob's group is working on cyber efforts to identify advanced degree disciplines. The website is divided by disciplines. They have emphasized cybersecurity and privacy.

## The annual meeting with stakeholders in academia is coming up next week on August 29th. It is an adobe connect webinar that previews the program for the next year including what's new for 2019. The theme for the meeting next week is cybersecurity.

## The Presidential Management Fellows program solicits advanced degree students. From 6,000 applicants they select 400-500 as finalists. These finalists are eligible to post for positions. All agencies with in the Executive Branch and the Library of Congress can accept applicants from the program.

## Are there plans to expand? The program is only available for federal civil servants. States can opt to have their own programs.

## Is there specific training for cybersecurity or IT? Training provided relates to current or targeted positions. There is 160 hours of training with an instructor and a developmental assignment lasting 4-6 months.

## Is funding for SFS being expanded? The program office will try to find out.

## Find out more [here](https://www.pmf.gov/agencies/value-proposition-and-overview.aspx).

## **Cybersecurity Labor Market and Statewide Survey**

## Eileen Sanchez presented on the cybersecurity labor market and the statewide [California Advanced Supply Chain Analysis and Diversification Effort (CASCADE)](http://business.ca.gov/Portals/0/Files/CASCADE/cybersecurity-labor-market-analysis.pdf) survey for the State of California.

## Eileen spoke about the CASCADE initiative to improve supply chain security and to support and grow California's cybersecurity workforce. The initiative is funded by the Department of Defense.

## How can the supply chain in CA implement cybersecurity? There is work in three main areas: Knowledge Sharing, Research and Analysis, and Education and Outreach. The hope is to develop workforce programs for supply chain.

## There were three goals for the study: Map the cybersecurity workforce demand, identify education and training programs, and provide a comprehensive report.

## There were also defense sector-oriented goals to help defense workers change over to cybersecurity.

## In CA, there are 35,000 job openings as of March 2018. Cybersecurity job postings have grown 3 times faster than IT job postings. The median salary for cybersecurity positions is $75,000.

## The first part of the study was to do demand research with cyber worker employers. Half of those surveyed were defense contractors. The NICE 2017 conference greatly aided in being able to complete this research. The NICE framework was the foundation of the study. They used nine work roles identified in the framework.

## The report includes profiles for each work role in the study. It also shows projections for the future for the work role.

## They are projecting an increase in the overall number of cybersecurity roles of all types in the next nine months by over 21,000 positions in CA. Most employers reported difficulty in finding people to hire. Defense contractors had great difficulty in hiring.

## Lack of qualified candidates, lack experience, lack of IT skills, and clearances were cited as challenges when hiring. They found that most work roles studied had an increased percentage of time spent in dealing with cybersecurity issues in the last 12 months.

## The study used the list of skills in the framework. Employers rated the importance of skills for roles in their business. Eighty percent or more of those surveyed indicated skills were important or very important.

## The Integrated Postsecondary Education Data System (IPEDS) is the source for identifying college and university cybersecurity education providers. The latest data available (2016) demonstrates there is a low rate of awards in cybersecurity-focused programs at that time.

## [CyberSeek](https://www.cyberseek.org/) estimates current job openings at over 35,000. The current supply is at about 13,000 candidates, meaning there is a deficit of approximately 19,500 workers. A more realistic interpretation of the numbers would show thirty-five thousand openings with an under-supply of 32,000 cybersecurity workers in CA. Education programs must greatly expand capacity to meet this demand.

## They are looking to employers to use the NICE Framework.

## Please email [Eileen Sanchez](mailto:Eileen.Sanchez@gobiz.ca.gov) with any questions.

## See presentation attached and find out more [here](http://business.ca.gov/Portals/0/Files/CASCADE/cybersecurity-labor-market-analysis.pdf) .

# Summary of Action Items

## Meeting minutes along with the presentations will be sent to members.

## The Program Office will investigate SFS grant funding status and respond to the members.

# Next Meeting Reminder - The next meeting is scheduled for September 26, 2018.