**NICE Working Group**

# Meeting Minutes

**Date: 6/28/2017 Time: 3:30 PM EST**

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

## Introduction and Ground Rules

* + Danielle Santos, NICE Program Manager, welcomed members 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 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 NICEWG is not intended for advertising and promotional purposes and to keep this in mind when participating and using the chat feature.

## NICE Program Office Updates

* + Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE), thanked everyone for joining and encouraged participation and engagement during the meeting.
	+ The NICE Program Office has been particularly busy with the summer conference season.
		1. The National Cyber Summit took place from June 6th – June 8th in Huntsville, Alabama which NICE helps support through a grant.
		2. The Colloquium for Information Systems Security Education (CISSE) held its annual conference in Las Vegas, Nevada from June 12th to June 14th. Davina Pruitt-Mentle, NICE Academic Lead, was in attendance and presented at the conference.
		3. Marian Merritt, NICE Lead for Industry Engagement, attended the Society for Human Resource Management Conference and Exposition (SHRM) last week to discuss how NICE can better engage with HR personal.
		4. The 2017 Community College Cyber Summit (3CS) kicks off this week in Largo, Maryland. Rodney will be in attendance on Friday, June 30th.
	+ A reminder that the NICE website is up and running with the recent addition of the NICE Working Group subgroups pages. Take a look and let us know what you think! <https://www.nist.gov/itl/applied-cybersecurity/nice>
	+ NICE released a Notice of Federal Funding Opportunity for Cybersecurity Education and Workforce Development Stakeholder Engagement Program. Interested parties are encouraged anyone to apply. Additional information can be found through the following link: <https://www.nist.gov/news-events/news/2017/05/notice-funding-opportunity-cybersecurity-education-and-workforce>

## Opening Remarks

* Industry Co-Chair, Andre Thornton, welcomed members to the call. Andre noted that artificial intelligence is becoming more and more of a reality. The takeover of jobs by automation is increasing. However, skills associated with creativity and emotional intelligence are the most difficult to duplicate in the artificial world. Andre believes creativity as a skill set is very important in the cybersecurity world.

## Standing Items

* **Metric Moment** – Jane Irwin presented on Year Up’s Cybersecurity Students
	+ 1. Year Up is a one year training program that typically works with students’ right out of school or people who are out of work. The program provides six months of professional training in IT, Financial Operations, Sales and Customer Support, Business Operations, or Software Development. At the end of the training period trainees then move onto a six month corporate internship with a respected company.
		2. The company was founded 17 years ago. Three years ago the company decided to be more market responsive by developing a cybersecurity piece. The cybersecurity pathway was launched in 2014. As new pathways are launched, the company tracks and collects data to keep an eye on the relevancy of their training. Due to successful outcomes they have expanded the program to DC, Phoenix and Chicago.
		3. In July of 2015 their first set of cybersecurity trainees graduated. The outcomes from cybersecurity internships compare favorably to Year Up’s outcome targets and to outcomes from other types of internships.
		4. In order to ensure that their students are meeting market demand, Year Up looks at the conversion rate: how many of those companies providing the internships are hiring their students. Year Up’s average conversion rate was 35% but was raised to 50% after the customized cyber training began.
		5. The retention rate of students who start the program and graduate under the cyber program can be equally compared to the other programs. The percentage of interns who graduated in 2015 was 84%. The percentage was 95% in January 2017.
		6. A member inquired how Year Up gets employers to commit to providing internships. Is it easy or challenging?
			1. It is important to gain corporate partner engagement through targeted meetings before launching in an area. Anecdotal evidence will back up market research which provides confidence in our partners.
			2. Cybersecurity is unique. While there is an obvious skills gap, the company found early on that most companies have small cybersecurity teams and not a lot of entry level jobs. However, this is still one of the tracks with the highest conversion rate. Most companies they work with are still trying to figure out what an entry level cyber employee looks like so this works well for them.
		7. Year Up has approximately 30 industry partners in addition to university partners. They are also partnering up with community colleges for training.
		8. See attached presentation and find out more here:
		<http://www.yearup.org/>
	+ **Fun Facts** – Alina Aragon presented on Summer Vacation Fun Facts.
		1. Alina sited information from a WTOP article which noted that some of America’s top Executives worked summer jobs like cutting tobacco or working at McDonalds. However, today’s teens are more likely to enroll in summer school, do volunteer work or do extracurricular activities.
		2. 1 in 5 Americans will go into debt to pay for summer vacation. Millennials may spend more but Generation X and the Boomers spend more with credit cards.
		3. DC has the most workers with unused vacation days amounting to 17 million. San Francisco comes in second with 12 million and Los Angeles with 3 million.
		4. See the attached presentation and find out more here:
			1. [http://wtop.com/life-style/2017/06/ceos-recall-when-teens-like-them-actually-worked-summer-jobs/](http://wtop.com/life-style/2017/06/ceos-recall-when-teens-like-them-actually-worked-summer-jobs/%22%20%5Co%20%22WTOP%20Summer%20Jobs)
			2. [http://www.magnifymoney.com/blog/news/1-5-americans-will-go-debt-pay-vacation1280032498](http://www.magnifymoney.com/blog/news/1-5-americans-will-go-debt-pay-vacation1280032498%22%20%5Co%20%22Summer%20Vacation%20Debt)
			3. <http://dcist.com/2017/06/dc_tops_under_vacationed.php>
	+ **Report Roundup** – Steve Curren reported on the ‘Health Care Industry Cybersecurity Task Force Report’
		1. The U.S. Department of Health and Human Services is typically focused on health care and emergency response. However, they are increasingly focused on the issue of cybersecurity.
		2. In the past three years there have been more cyber breaches than ever. Currently, a multitude of countries in the world are in the middle of a fairly significant ransomware attack. The Wanna Cry ransomware attack last month severely disrupted 3 to 4 healthcare facilitates in the United Kingdom.
		3. In 2015 Congress passed the Cybersecurity Act of 2015 and established the Health Care Industry Cybersecurity (HCIC) task force to address challenges the health care industry faces when securing and protecting itself against cybersecurity incidents.
		4. The task force convened experts to look at the issue of cybersecurity from the private sector perspective. The group met for a year and put together a report with 106 recommendations for the sector. About half of the recommendations are directed toward HHS and the other half are for the industry to take actions on. The information was organized under 6 imperatives:
			1. Define and streamline leadership, governance, and expectations for health care industry cybersecurity.
			2. Increase the security and resilience of medical devices and health IT.
			3. Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
			4. Increase health care industry readiness through improved cybersecurity awareness and education.
			5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
			6. Improve information sharing of industry threats, risks, and mitigations.
		5. Rodney inquired about education and workforce provisions and whether there is anything unique to this industry? The task force thinks there are several unique factors in health care; health care falls under HIPPA and the Health Care Act. The Healthcare Industry is the largest target.
		6. See attached presentation and find out more here:
		<https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>
	+ **Event Engagement** – Kristi Horton presented on ‘Sector Coordination and ISAC Events’
		1. ISACS are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators. The organization was born out of a presidential order in 1999, established to coordinate information sharing with regards to physical and cyber threats for industries such as water, oil, healthcare, automotive, facilitates, etc. Organizations coordinate with one another and with the government itself. The National Council of ISACs coordinates between the ISACs themselves and also with the government. Kristi is an analyst and a real estate ISAC and also participates with the National Council.
		2. Kristi noted that two questions were posed to ISAC members. The first question: how can we engage in some of the events ISAC has coming up? Members responded that they list their events on a public facing website. The second question: what efforts are you doing in your sectors toward cybersecurity education? Some responded that they have members who have formed a committee and are looking at providing training within member organizations. One even hired a manager to build out a training program for their members.
		3. Rodney asked if there are specific opportunities for better engagement with the NICE community along with the critical infrastructure community. Kristi believes there are direct ways the NICE working group can engage the ISACS. Kristi was an employee of the Financial Services ISAC where much of the subject matter is around cybersecurity. A lot of the members present concept research or case studies so that they can each learn from one another’s experiences. But, she does not believe anyone has put together a gap analysis to see what skills are missing, especially with respect to the threat landscape. Here is an opportunity to look at what they do need and how to fill in the gaps.
	+ **Strategy Stories** – Rick Howard, Palo Alto Networks, spoke about the Girl Scout Cybersecurity Badge Program. This topic supports 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.
		1. Women make up less than 14% of the cybersecurity workforce. When looking at minorities within that group the number drops to 1%. There are a multitude of reasons why girls/women lose interest in STEM studies, such as the male dominated culture and a lack of attainment.
		2. Palo Alto Networks partnered with the Girl Scouts organization to build a cybersecurity badge program for K-12. There are two categories, 1) online safety and 2) network defender.
		3. Almost two million girls will receive training to become experts and leaders in the field.
		4. Palo Alto Networks has received a tremendous amount of requests for help and support.
		5. A member inquired if other organizations can get involved? Rick said for anyone interested to email him and he will get them connected to the appropriate people. rhoward@paloaltonetworks.com
		6. Find out more here: <https://www.paloaltonetworks.com/company/press/2017/palo-alto-networks-and-girl-scouts-of-the-usa-announce-collaboration-for-first-ever-national-cybersecurity-badges.html>

## Subgroup Updates

* + **K-12** - Carlos Garcia, co-chair, provided the K-12 update.
		1. Carlos announced that he recently accepted a new position at Jackson College in Michigan as the Lead for Cybersecurity.
		2. Twenty new members have been added to the K-12 group in the month of June.
		3. During their last meeting they discussed the 2017 K-12 Education Conference and have recruited new members for the two project teams.
		4. Rodney Petersen provided a presentation on the President’s Executive Order on Cybersecurity and asked for feedback from the subgroup.
		5. Members have been collecting resources from across the U.S. with the intent to have two reports shared by K-12 members at the conference.
		6. The K-12 group have been working on their charter updates in order to align with all of the NICE subgroup charters.
		7. Cybersecurity Awareness Week information will be hosted off of the NICE website. Members are also looking at deliverables and other ideas for activities.
		8. The July K-12 meeting has been canceled. The next meeting is scheduled for August 9th.
	+ **Collegiate** – Heather Monthie, co-chair, provided the Collegiate update.
		1. The tools, technologies, and skillsets project team led by Stephen Miller is researching tools and technologies to demonstrate student skillsets. This team is looking at mechanisms for job seekers to connect with employers. They are putting together a framework portfolio for students and working to develop a toolkit. [Cyberstudents.org](https://www.cyberstudents.org/) may be a good way to disseminate the work. The group is hoping to have a face to face meeting during 3CS this week.
	+ **Competitions** – Jessica Gulick, co-chair, provided the Competitions update.
		1. The Competitions group has recently had a number of new members join.
		2. Selected members were recently at CISSE and talked about how competitions add value to education and helping people find jobs. There are a couple more events planned in the near term.
		3. The group has been discussing how to restructure the monthly meeting to introduce a tool and technology speaker to provide information to the members. New resources will be added to the website.
		4. Members would like to hold a leadership conference in parallel with the NICE Conference to bring members together to talk about what direction to take into the future.
	+ **Training and Certifications** – Linda Montgomery, co-chair, provided the Training and Certifications update.
		1. Twelve new members were added in June.
		2. The Skills Based Performance group, led by Doug Rausch, has been responsible for establishing a methodology of standards and measurements. A big part of the effort was determining definitions so that we are all using the same language. This effort was completed in May. Members are now looking at performance based assessments, tying back to NICE Strategic Plan Goal 2, which will be in progress for some time.
		3. The Framework to Certifications Group, which aligns with the NICE Strategic Plan Goal 3, will apply the developed standards to the mapping matrix. The framework of that document has been completed and they are now discussing how to proceed with mapping to work produced by C3. Once the mapping is complete they will be able to identify the gaps at which point the Supply and Demand/Training Gap team will embark on analysis.
	+ **Workforce Management** - Kristin Judge, co-chair, provided the Workforce Management update.
		1. The KSA project continues to grow and move forward.
		2. The most recent project work is the development of a reference construct for contributing and mitigating cybersecurity risk by functional areas within an enterprise. Seven different functional areas and the positions where impacts are most felt have been developed. These seven areas include: Planning and Governance, Facilities and Operations, Information Technology, Legal and Compliance, Human Capital, Finance and Admin and Sales and Marketing. Teams are forming based on the business areas. Kristin invites anyone with expertise that aligns to these areas to assist with the work.
		3. To participate in one or more areas, or share your perspective so that we can be sure we are developing prescriptive guidance please contact the co-chairs. We look forward to your participation.
		4. The Human Factors Project Personas Template slides are available within the Workforce Management subgroup site on SharePoint.
		5. Contact the co-chairs here: muenuma@tripwire.com, kristin@staysafeonline.org

## 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 will be participants from the Department of Education and the First Lady of the State of TN. Keynote speakers are currently being confirmed.
		3. Conference mailers will go out once all the speakers are confirmed. There will be some unique panels, such as student panels on how to inspire a workforce. Registration should be launched at the end of the month.
		4. The conference committee is reviewing submissions.
		5. Find out more here: <https://www.k12cybersecurityconference.org/>
	+ **NICE Annual Conference - Danielle Santos**
		1. The keynote speakers have been announced.
			1. Rob Joyce, Special Assistant to the President, Cybersecurity Coordinator
			2. Moderating the CISO panel is Arik Perminter, President of the International Consortium of Minority Cybersecurity Professionals
			3. Angela Messer, Executive Vice President, Booz Allen Hamilton Cyber Innovation and Talent Office
		2. There are three pre-conference seminars confirmed for this year which require a separate registration. 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
		3. Proposals that have been received are under review. Announcements should come out next week. An agenda will be populated after confirmations.
		4. There will be one keynote speaker from the military, Major General Mark E. Bartman, Ohio National Guard Adjutant General.
		5. Registration is now open! Find out more here: <https://www.fbcinc.com/e/nice/default.aspx>
	+ **NICE Challenge Project – James Ashley, Project Manager**
		1. The team has been present demonstrating the project at conferences such as the Information Assurance Symposium, National Cyber Summit and 3CS.
		2. The NICE Challenge Project now has over 100 officially registered educational institutions in the U.S.
		3. The project is expected to have some major releases this summer including the official 1.0 release of its web application, taking it out of beta, as well as a new challenge environment. There will also be another release later this fall.
		4. There are now 60 plus challenges available within the Operate & Maintain challenge environment.

Find out more here: [https://www.nice-challenge.com](https://www.nice-challenge.com/)

## New Business

* + Rodney Petersen spoke about the “Workforce Provisions of the President's Executive Order on Cybersecurity”
	+ The NICE Program office has been busy developing a response to the executive order. More information on the executive order can be found by listening to the recorded NICE webinar here: <https://www.nist.gov/news-events/events/2017/06/presidents-executive-order-cybersecurity-workforce-next-steps-and-how>

While there are four parts to the executive order, one specifically directs NICE to do two things:

* + 1. Assess the scope and sufficiency of efforts. Work on this effort is ongoing. In addition to Alina joining the team we also have two post-graduate fellows reviewing and performing an environmental scan.
			1. A Request for Information (RFI) is expected to be released any day now. The Program Office asks working group members to look for the RFI and provide information into the process. The RFI has a few open ended questions. Contributors can especially identify any promising programs not yet considered or make recommendations that have been made before but adding new ideas as well.
			2. While other agencies have been identified to assist with these efforts, our awareness of programs and initiatives will create a comprehensive assessment.
		2. Provide a report to the President within 120 days with findings and recommendations. The RFI asks for input, especially recommendations. The Program Office is reviewing old recommendations but also looking for new ideas for innovation and change. The ultimate deadline is September 8th.
	+ Rodney believes the assessment of scope is straight forward. The environmental scan is intended to be as comprehensive as possible. Metrics are significant and show how we define impact would add to the importance. Also, there is an importance to not only sustain the cybersecurity workforce but recruit as well.
	+ There are a variety of programs and initiatives already in place or being built that should be shared. Demonstrating success of our programs is also key, reminding people of the NICE values to ‘Seek Evidence’.
	+ The sustainment and growth of the cybersecurity workforce is important. How do we maintain a steady growth state and retain developed skills appropriately?
	+ The Program Office is looking at national, local and regional efforts and also has an international component that will look at cybersecurity competitiveness. NICE is also looking at international cooperation around education and workforce development.
	+ Inquiries can be made here: Cybersecurityworkforce@nist.gov
	+ Find out more here: <nist.gov/nice/cybersecurityworkforce>
	+ The website will add a link to the RFI once it becomes available.

## Summary of Action Items

* + Minutes and presentation materials will be sent to all members.

## Next Meeting Reminder

* + The next NICEWG meeting is scheduled for July 26, 2017