**NICE Working Group**

**Meeting Minutes**

**Date: 2/28/2018 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 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.

# 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.

# NICE Program Office Updates

# Rodney Petersen, Director of the National Initiative of Cybersecurity Education, welcomed members to the February meeting.

# As the season begins to change, it serves as a reminder to focus on new growth. NICE hopes we’ll all become a bit more active to identify progress and change.

# Goals and objectives are undercut by values. The NICE Strategic Plan outlines a few values that speak to challenging assumptions. There is a lot of progress being made and a lot of room for improvement. This is a good time to remind ourselves to innovate. Now is a great time to continue to promote and uphold those values.

# Other values, such as pursuing action, sharing resources, remind us to reach out to peers and work collaboratively. Throughout today for example, members of the NICE team just finished meeting with the CIO Workforce Committee.

# Moving forward, we experience progress and change yet are seeking evidence to measure results that show outcome. Also of great importance is the inclusion and importance of diversity. Rodney is reinvigorated by all the working group members.

# Standing Items

* **Report Roundup**   
  Jon Oltsik, Senior Principal Analyst, ESG, presented on “The Life and Times of Cybersecurity Professionals”

1. The Enterprise Strategy Group (ESG) Information Systems Security Association (ISSA) research report is a free download.
2. In summary, the survey is a quantitative web-based survey using ISSA members who are cybersecurity practitioners all over the world. This is the second annual report. ESG is striving to acquire trending data.
3. 70% of those surveyed say the shortage of cybersecurity workers has had an impact on their organization. Organizations are impacted with increased workloads, emergency issues only resolved, the lack of opportunity to provide ongoing training, and a lack of strategic planning.
4. Respondents stated that skills shortages are prevalent for security analysts, cloud security specialists and application security specialists.
5. Ongoing efforts to automate and to document and formalize cybersecurity processes are needed to take over manual processes.
6. The gap between business and cybersecurity may be closing but people who want good enough security and is not a business concern.
7. A high percentage of respondents strongly agreed that cybersecurity professionals must keep up with their skills or the organization is at a risk. It is difficult to keep up with skills due to the high demand of the job; there is no time for ongoing training which represents a threat.
8. When asked if your organization provides the right level of training, 38% say yes but this means other organizations should be providing more or significantly more training. This is another red flag.
9. The most effective methods to increase KSA’s are one, cybersecurity training, and two, participating in professional organizations within their industry and profession. Results show a consistent over emphasis and hard selling on cybersecurity certifications. Certifications are not the most effective way to increase knowledge. People over-emphasize certifications which have a marginal return.
10. 49% of professionals are solicited by headhunters and such to get another job. This does not equate to a healthy market. For the professional, the average increase in salary is 20% from job to job.
11. There is a combination of things that should happen in managing a career. In looking at the life cycle, professionals are not actively managing and developing their careers while employers are not mentoring them.
12. Money is always important to build a center of excellence. Organizations must support training and must implement a cultural commitment to support the cybersecurity professionals who want to work with others that are very talented. They also want the ability for career advancement.
13. Feel free to look at the report and send questions or comments to Jon.
14. Jon is presenting at RSA on Thursday, April 19 around 9:00 AM. The schedule will be shown on the calendar.
15. See attached presentation and find the report [here](mailto:https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/surveyes/ESG-ISSA-Research-Report-Lif.pdf).

## **Strategy Stories** Brian Payne, Chair, HRCyber, presented on the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber). This effort aligns with the NICE Strategic Plan Objective 3.3: Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

1. HRCyber, supported by NICE, along with other partners across the region, are making some great strides building cybersecurity educational pathways and professional development.
2. HRCyber works with industry and non-profit partners. Those involved made efforts to sit down and listen to what we’re doing well and what cybersecurity students should be taught. Comparisons between industry and faculty were made and the results are to rethink how we’re executing things.
3. Students benefit greatly from hands-on experiences. This is already known but still helpful listening to what industry is saying.
4. Changes in the academic field have been made. Internships have become a requirement and a major in the college of business on enterprise cybersecurity has been developed. Also developed is a virtual lab that brings together community colleges and universities as well as articulation agreements that make it easier for students to move between higher education institutions.
5. Listening to partners and then implementing ideas has been very important. Industry opened their doors and we continue to find ways to sustain these efforts.
6. HRCyber is now developing the HRCyber lab, supported by a grant and dollars from businesses to help build on current efforts. The lab will include aspects like cyber-arena where industry partners can test cyber materials and products.
7. Cyber trail is an effort to initiate efforts across Virginia to become a statewide initiative and to connect researchers.
8. Part of the digital entrant pillar is an internship program providing more funding for business to test new employees. We will subsidize a percentage of the employee salary for the first year then businesses decided to hire after a year or not. The money goes back to the co-lab if that employee is hired.
9. See presentation and find out more [here](http://securitybehavior.com/hrcyber/).

## **Metric Moment** Marshall Criser III, Chancellor, State University System of Florida, presented on the University System of Florida Performance-based Awards.

1. The performance-based funding model began in 2014. The model is based on four guiding principles and key components that balance both risk and awareness.
2. Monetary investments are from both institutions and from the state.
3. Excellence and improvement are recognized.
4. Ten key metrics were developed incentivizing student success. Focus on access.
5. Many factors are reviewed and tracked. Some include cost to student, wage when entering workforce, post-graduation jobs and continuing education. Cost of education vs. salaries of students following graduation when they enter the workforce are also evaluated.
6. Graduation rates have increased since performance based funding was implemented.
7. There is a focus on a metric chosen by the board of trustees to find balance between success and recognizing individual universities.
8. The Board of Governors designated each state research university that meets at least 11 of 12 academic & research standards set in statute as a “preeminent state research university’ to be eligible for funding.
9. As the universities develop more degrees there is the opportunity to contribute to student’s success. There is effort to continue to develop a separate category for cybersecurity though team grants. Strategic shortfalls in comp science have been identifies and increased direct funding has increased enrollment.
10. A member asked how student success is defined. By looking at percentage of students that are employed a year out and those that seek continuing education. They look at average earnings of students. An undergrad follow-up study to track real student placement from degree to job is in place.
11. Students can be influenced by continuing to work closely with them and by leveraging the alumni centers to assist in recruiting.
12. See presentation and find out more [here](http://www.flbog.edu).

# New Business

## Matt Bishop, University of California, Davis, presented on cybersecurity curricular guidelines

1. Version 1.0 of the Cybersecurity Curricula 2017 has been officially released and endorsed.
2. This body of work took 2.5 years and had 3 public review iterations. Over 325 people contributed covering persons from most continents.
3. Guidelines organized around 3 principles including the vision, mission and goals.
4. The body of knowledge areas include technical and non-technical.
5. Exemplars support different kinds of programs. This is a living area, adding more as we go along.
6. Within each knowledge area there is a detailed description. At the end of each, is a list of key points that the working group feel are most critical.
7. The context of this document includes guidelines. Different schools have different strengths.
8. Guidelines were developed so people can take what they have and improve. Bodies can use the guidelines to develop criteria.
9. There is a relationship between guidelines and accreditation.
10. When developing certifications, the guidelines can be used to see what should be covered; after, decide the depth to cover.
11. The focus is on hostile environments for guidelines. Groups felt not due to an attack. If failed during an adversary your facing something hostile.
12. There are plans to speak and present at many upcoming conferences.
13. The file can be downloaded from the website [here](http://cybered.acm.org/).

# Subgroup Updates

* **K-12**

### Kimberly Henderson, San Jose State University, provided the K-12 update.

1. During the last K-12 subgroup meeting, there were two presentations:
   1. Gustavo Hinojosa, Executive Director, presented on the National Cybersecurity Student Association (NCSA).
   2. Cassi Elliott*,* Regional Marketing Manager at Oracle, provided information about the Oracle Academy.
2. Members provided ideas and discussed the creation of one pagers and info graphics.
3. Developing ideas for curricula was also discussed. Currently, there is no Advanced Placement (AP) credit in cybersecurity for pre-college students. The goal to develop an AP credit program in cybersecurity is on the radar. Processes for creating new AP credit programs with the College Board are complex and will take time to develop.
4. The next subgroup meeting is on March 14, 2018

* **Collegiate**

Rodney Petersen provided a brief update for the Collegiate subgroup

1. There are two project teams within the subgroup: Academic and Career Pathways, and the Tools, Technologies, and Skillsets groups.
2. The Academic and Career Pathways team are looking at pathways starting from the Collegiate level down and beyond.
3. The Tools, Technologies, and Skillsets team is looking at different tools, technologies and skillsets required for cybersecurity jobs to provide those tools online through a portal. The portal will connect students with a sponsor and a mentor. The portfolio and portal as well as a white paper will be the project deliverables. They are currently trying to find sponsors so that they can offer the portal for free to students. They also need to find mentors to help with the review
4. Members interested in participating on these projects can reach out to the co-chairs ([Stephen Miller](mailto:stephen.miller@enmu.edu); [Heather Monthie](mailto:heather.monthie@gcu.edu)) or [Rodney Petersen](mailto:rodney.petersen@nist.gov).

* **Competitions**

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

1. The Competitions subgroup met last week. The group is developing recognition letters for competition winners. Katie Hanson has developed the first draft. The team is also working on coordinating the process.
2. The first in a series of podcasts on cyber competition has been published on the [CyberCompEx](https://www.cybercompex.org/) website. CyberPatriot is discussed with Allen ​Stubblefield. Allen is also presenting during the next Competitions meeting on March 22nd. The next podcast is coming in the next month.
3. Project teams are developing instructions on how to build and run a competition, and a guide for competitors. A draft is available on how to build and run a competition. There is discussion on how to potentially advance the guides into a summer workshop.
4. Members are also reviewing the current competitions one pager wondering if it addresses all stakeholders. There is discussion on including a workforce component.
5. There is a desire to get information on competitions into middle schools and building out cross team collaboration with the K-12 subgroup.

* **Training and Certifications**

### Linda Montgomery, co-chair, provided the Training and Certifications update.

1. The Skills Based Training project team will continue to look at methodologies established in 2017 on an as-needed basis. The team will drill down and identify three major components which are tied to the NICE Strategic Plan.
2. The Framework to Certification project team is using the methodologies and standards developed by the Skills-Based Training working group. The mapping matrix and is out for an internal review and will be provided to a larger audience for more input. The team has mapped works roles to specialty areas. Later, proficiency levels will be brought in.
3. The Supply and Demand Training Gap project team is looking at how to build a template for communities to reach a market level such based on the work happening in San Diego.
4. Members discussed and agree to bring back the Cyber Range project team. They are looking for individuals to join this group to co-lead. Identifying criteria and taxonomy of a range, identify tools and resources are a few of the topics to research.
5. Please reach out to [Linda Montgomery](mailto:lmontgomery@tlclasvegas.com) and [Ken Slaght](mailto:ken.slaght@sdccoe.org) if interested.

* **Workforce Management**

### Maurice Uenuma, co-chair, provided the Workforce Management update.

1. NICE Working Group members received an email on February 27th outlining instructions to review the draft of "The Resilient Workforce: Cybersecurity is Everyone’s Job". The guidebook was a major project focus area of this subgroup which has moved through several iterations. The guidebook is Intended to be consistent with the [NICE Strategic Plan](https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/strategic-plan) Goal 3.4: to promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals. The guidebook is intended for hiring managers and leadership within an organization to guide their workforce effectively and to reduce cybersecurity risk.
2. The guidebook is intended to be a set of cybersecurity guidelines for everyone in an organization. Everyone must be involved in addressing cybersecurity. Risk must be addressed across the entire workforce, including the supply side. The book is written for a non-IT, non-cybersecurity oriented audience. It is an introduction to the topic, written in plain English.
3. To help us get a sense if this will hit the mark or not, general and specific comments are welcome. Feedback on the current draft will be accepted through March 21st. Revisions can be uploaded to the [SharePoint](https://nistgov.sharepoint.com/sites/NICEProgram/NICEWG/WorkforceManagement/Shared%20Documents?viewpath=%2Fsites%2FNICEProgram%2FNICEWG%2FWorkforceManagement%2FShared%20Documents) site, or returned by email (make changes in Track Change mode, and send via email to Editors Susie Cone ([susie.cone@gmail.com](mailto:susie.cone@gmail.com)) and Maurice Uenuma ([muenuma@tripwire.com](mailto:muenuma@tripwire.com)).
4. To provide feedback, please download the attachment or access the same file on our SharePoint site (<https://nistgov.sharepoint.com/sites/NICEProgram/NICEWG/Pages/home.aspx>)
5. A public comment period will follow the working group review period and assimilation of comments received.
6. Thanks to all who have provided comments thus far.
7. A member commented that the tag line uses “job” and asked the reason for this. Maurice stated that the use of "Cybersecurity is Everyone's Responsibility" is used for National Cyber Security Awareness Month. This comment will be taken into consideration this for the next version.

# Project Progress Reports

* **CAE Community**

Anastacia Webster, California State University, San Bernardino, provided an update.

1. During the week of March 5th, the website will have a soft launch. Links to the site and instructions on how to comment will be sent. Prior to a full launch, updates will be implemented based on feedback.
2. The CAE virtual career fair is scheduled for October 5th, 2018. Organizations will have the ability to meet the talent the CAE community is producing.
3. Find out more [here](https://www.caecommunity.org/).

* **NICE K-12 Cybersecurity Education Conference**

Davina Pruitt-Mentle, NICE Academic liaison, provided an update.

1. The location for the Cybersecurity Education Conference will be the Grand Hyatt Hotel in San Antonio, TX.
2. The first conference planning committee meeting is coming up in March.
3. The conference is scheduled for December 3-4, 2018.
4. Find out more [here](https://www.nist.gov/news-events/events/2018/12/2018-nice-k-12-cybersecurity-education-conference-save-date).

* **NICE Challenge Project**

James D. Ashley III, Lead Engineer | Project Manager, provided an update.

1. System capacity and usage have increased significantly this year.
2. Monthly webinars and other marketing will continue to further increase capacity.
3. Next month, the re-designed player work flow on challenges will be available.
4. The new protect and defend environment will be online next month.
5. Find out more [here](https://nice-challenge.com/).

# Summary of Action Items

* Review the Workforce Management guidebook. The deadline is prior to the next working group meeting.
* RSA speakers can provide their speaking information to be added to the minutes if the topic is related to NICE.
* Please inform the NICE Program office about any upcoming events.
* Minutes and presentation materials will be sent to all members.

# Next Meeting Reminder – the next NICEWG meeting is scheduled for March 28, 2018.