**NICE Working Group**

**Meeting Minutes**

**Date: 5/24/2017 Time: 3:30 PM EST**

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

1. **Roll Call 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.
* 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.

1. **NICE Program Office Updates**

* Bill Newhouse thanked everyone for joining as well as the speakers for sharing information about their work toward the progress of the objectives within the NICE strategic goals.
* Bill informed the group that there is a grant opportunity available to allow an entity to assist in developing future NICE conferences and encourages anyone interested to apply. Additional information can be found at: [www.grants.gov](http://www.grants.gov).
* All slides and materials will be made available after the meeting.

1. **Opening Remarks**

* Industry Co-Chair, Andre Thornton, welcomed members to the call.

1. **Standing Items** 
   1. **Fun Facts** – Kristin Judge, National Cybersecurity Alliance, spoke to the “Dell End-User Security Survey”.

* The survey was conducted online during late February through March 2017. Over 250 workers were surveyed. The survey found:
  + 46% of employees admitted to connecting to public Wi-Fi to access confidential work material.
  + 49% admitted to using personal email accounts for work particularly because it is easier to use and it allows them to get around perceived time consuming safety measures.
  + 35% admitted to taking corporate information with them when leaving a company.
  + 72% were willing to share confidential company information without caring about the security protocols.
  + 65% of employees recognize their responsibility to protect work information but find the security programs limit their productivity.
  + Of employees who have received cybersecurity training 24% admitted to using unsafe behaviors in order to complete a task.
  + There is a great need to create a culture of cybersecurity awareness. Best practices need to be taken out of IT and into risk management. Security should not hinder the day-to-day of a business, but support the work through a closer alignment between an organization’s C-Suite and IT Teams.
  + The Human Factors Team within the Workforce Management subgroup is looking at how to create organizational change where everyone understands their security role within the organization.
  + See attached presentation for more information and find out more here: [http://dellsecurity.dell.com/wp-content/uploads/2017/04/2017-Dell-End-User-Security-Survey\_FINAL.pdf](http://dellsecurity.dell.com/wp-content/uploads/2017/04/2017-Dell-End-User-Security-Survey_FINAL.pdf%20)
  1. **Report Roundup** –Dan Waddell, ISC2, spoke to the ‘State of Cybersecurity (ISC)2.
* This presentation was originally presented at the CyberSecureGov 2017 event on ‘Educating the Workforce in Cyber’.
  + The study specifically focused on federal government employees. It is the 8th version of the bi-annual study and the largest study of information security ever conducted. The results provide a good cross cut across the entire workforce. The sample size of the study was 2,620 federal workers with 1,614 being in the military and 1,006 in non-military. The average participant age was 47. They have been working with high school, university and academic partners to bring down the average age. Only 15% of the participants were women. The organization is trying to make a concerted effort to reach out to underrepresented groups. Nearly half of the participants reside around DC.
  + The respondent profile shows that the average salary for respondents is $118,000. The top three job positions listed are information assurance manager, security analyst and security engineer.
  + The study shows that keys to retention are training and certification, better compensation and flexibility. If the government is willing to pay for certifications then people will stay longer. Thus, retention is not always about higher pay.
  + The keys to attracting new hires is certification, training and education. There are varying perspectives on what skills employees think they need and those that the hiring managers want.
  + 78% of respondents claim highest demand for new hires exist in the non-managerial staff segment. Federal executives don’t have the resources to train up but programs like NICE help build that bridge.
  + See attached presentation for more information and find out more here: [http://iamcybersafe.org/gisws/](http://iamcybersafe.org/gisws/%20%20)
  1. **Event Engagement** – Wendy Newton spoke to the Information Assurance Symposium.
* Wendy is a Program Manager for the Information Assurance Symposium.
  + The event is being held at the Baltimore Convention Center and Hilton Hotel in Baltimore, MD from June 19th to the 21st.
  + The event is a NSA premier information insurance event. There will be three primary tracks. Approximately 150 briefings will be made across the three days. The symposium is free to government employees. The fee is reduced for contractors and industry working with the government.
  + Registrants do not have to choose sessions in advance.
  + All symposium briefs are due this Friday, May 26, 2017.
  + See attached presentation for more information and find out more here: [https://www.fbcinc.com/e/ias/](https://www.fbcinc.com/e/ias/%20%20)
  1. **Strategy Stories** – Noel Kyle, DHS, spoke to new developments that align to the NICE Strategy. This topic supports the NICE Strategic Plan objective 3.4: Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals.
* Noel’s office promotes cybersecurity awareness, training and workforce development and have been working with NICE for a long time.
  + Noel walked through the NICCS (National Initiative for Cybersecurity Careers and Studies) website and talked about workforce development tools available to help build a workforce strategy.
  + Noel pointed to the Workforce Development Toolkit available online. The toolkit outlines four different phases: 1.) the Prepare Phase which assists to assess goals and evaluate readiness, 2.) the Plan Phase to assist with inventorying a workforce and ongoing workforce planning, 3) the Build Phase to help close the skill gaps and recruit for key skills and, 4.) the Advance Phase to provide guidance on staff retention and continuous development.
  + Ideally, this toolkit helps you get a feel for where your organization stands and what kind of workforce you have. Then, it provides guidance on building it out.
  + The NICE Framework is the foundation for all of their tools and resources. NICCS features the 2013 version (2013) of the NICE Framework.
  + Also available within the Workforce Development section is the Push Button PD Tool. They are currently on version 20. The tool assists in building a job description: the skills and knowledge requirements are entered and the tool will result in a position description. It will also result in the federal government form requirements as well.
  + There is a NICCS website training catalogue which was designed to be a one-stop shop. NICCS is working with 150 different training providers resulting in over 3,000 courses loaded onto the site.
  + Courses are added through an extensive vetting process with vendors. Vendors must demonstrate their alignment to the workforce framework.
  + Some of the resources on the education tab could be obtained by those in academia but for additional course information there would need to be further discussion with the NICCS office.
  + FedVTE (Federal Virtual Training Environment) offers free online and on-demand training courses 24/7. FedVTE is available to government employees and includes more than 60 courses with many aligned to cybersecurity certification exams. The classes range from beginner to advanced.
  + Please check out the site and feel free to contact the NICCS (niccs@hq.dhs.gov) office or Noel Kyle ([Noel.Kyle@hq.dhs.gov](mailto:Noel.Kyle@hq.dhs.gov)) with any questions.
  + See attached presentation for more information and find out more here: [https://niccs.us-cert.gov/workforce-development](https://niccs.us-cert.gov/workforce-development%20)
  1. **Metric Moment** – Melissa Dark presented on the Gen Cyber Program.
* Melissa is a faculty member at Purdue University but is also a contractor for the NSA evaluating the GenCyber Program.
  + The program is now four years old. There will be 132 camps this year at 82 different colleges and universities for both students and teachers. The prediction is that there will be approximately 4,000 students and 1,100 teachers. The GenCyber program has three main goals:
    - 1. Increase interest in cybersecurity and increase diversity on cybersecurity workforce.
      2. Improve safe online behavior.
      3. Improve the teaching and teaching methods of K-12.
  + The current metric is to look at student interest through retrospective questions: 1.) how much interest does a student have; 2) intention to act upon interest and; 3) the belief in your ability to succeed.
  + This year they will be doing a pilot study with a subset of camps and look at those indicators at both 6 and 12 months after the camp which will help to build up the GenCyber program. They will focus on the intention and belief to act as well as look at any obstacles.
  + The instrument will look at intended behavior and then develop and validate with approximately 800 people so the data can be used as a census next year.
  + They will also ask teachers their intention to use the material they acquired (how many lesson plans, how long and how many students they are reaching). This will be part of the impact study follow-up.
  + There are no plans to gather information from prior year students at this time.
  + See attached presentation for more information and find out more here: <https://www.gen-cyber.com/>

1. **Subgroup Updates**
   1. **K-12** - Virginia Lehmkuhl, Dakhwe, co-chair, provided the K-12 update.

* The last meeting was held on May 10th and included a presentation from the Hampton Roads RAMPS team who provided a brief overview of the multi-dimensional RAMPS effort.
* There were updates on the NICE K-12 education conference. Members also spoke about upcoming conferences they plan on attending.
* The subgroup discussed the work on Cybersecurity Career Awareness Day/Week. This effort is expected to take place from November 13-17.
* The team is proposing and compiling resources and thinking about the structure of the resources. There is ongoing work around the planning of this offline.
* The next meeting is scheduled for June 21st.
  1. **Collegiate** – Casey O’Brien, co-chair, provided the Collegiate update.
* This subgroup meets on the 2nd Tuesday of each month with the next meeting scheduled for June 20th.
* Currently the Collegiate group has two project teams.
  + The first is focused on academic pathways and is headed up by Kevin Powers.
  + The second is focused on tools, technologies and skill sets and is led by Stephen Miller. This team is looking at mechanisms for job seekers to connect with employers. One key activity planned is to review the National Students Cybersecurity Student Association and what they are doing.
* Please reach out to Heather Monthie ([Heather.Monthie@gcu.edu](mailto:Heather.Monthie@gcu.edu)) and Casey O’Brian ([cobrien@nationalcyberwatch.org](mailto:cobrien@nationalcyberwatch.org)) if interested in joining.
  1. **Competitions** – Dan Manson, co-chair, provided the Competitions update.
* Laurin Buchanan just completed a new document titled “The 10 Things Parents Need to Know about Cyber Competitions”. The document will be uploaded to the Competitions SharePoint site and added to the [Competitions page](https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group/competitions-sub-working-group) on the NICE website.
* The National Cyber League completed the spring season. There was a total of 891 individual players covering 43 states.
* CyberPatriot announced their camps of which there will be 105 in 160 locations.
* CyberPatriot set a record for the amount of days to get to 1000 teams and was able to surpass registered teams 37 days after launch of registration.
* Find out more here: [http://uscyberpatriot.org/Documents/2017%20AFA%20CyberCamps\_Approved%20List.pdf](http://uscyberpatriot.org/Documents/2017%20AFA%20CyberCamps_Approved%20List.pdf%20)
  1. **Training and Certifications** – Linda Montgomery, co-chair, provided the Training and Certifications update.
* The team has been working on the assimilation of data with C3. They are taking certifications and using the methodology of the NICE workforce framework, identifying key words to blooms cognitive action verbs to bring to the full spectrum and scope.
* The mapping brought not only the certification but also mapped to the proficiency level. There is much debate on how to settle on proficiency level.
* For tasks, curriculum and content of certifications are at the granular level. There is an ability to drill down to various areas and locate an overall correlation.
* This is the direction our project team is going. There is agreement on data points of where were heading with the three groups working in tandem. We look forward to sharing the final product with the larger working group.
* See presentation for more information.
  1. **Workforce Management** - Maurice Uenuma, co-chair, provided the Workforce Management update.
* This subgroup has been developing a guideline on integrating cyber security roles into functional areas within an enterprise.
* The team is taking a holistic look with the intended audience being non-technical.
* After developing the framework tool, the team looked at individual business functions and at the risks and mitigation for their roles. The information is turning into a reference document that can be used for the target audience.
* Discussion now centers on how to present the information and also provide resources in each of the functional areas (resourcing, training, etc.).
* The back side of the template is a tear sheet to provide individuals with resources and common tasks.
* In thinking about cybersecurity tasks a direct link was applied to the NICE framework as a taxonomy.
* The goal of this effort is to strengthen the cybersecurity posture of an organization.
* The project team is defining content for key roles and plans to reach back out to broader community in those functional areas.
* 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.
* See presentation and contact the co-chairs here: [muenuma@tripwire.com](mailto:muenuma@tripwire.com), [kristin@staysafeonline.org](mailto:kristin@staysafeonline.org)

1. **Project Progress Reports**
   1. **NICE K-12 Cybersecurity Education Conference**

* Amber Lindsay provided an update on the conference being held December 4-5 in Nashville, TN at the Omni Hotel.
* The call for speakers closes on May 31st. Submissions are encouraged!
* Registration will open on June 1st and an announcement will be sent out during the first week of June.
* Conference will feature hands on workshops to help create a dialog on how to inspire a career in cybersecurity.
* Find out more here: <https://www.k12cybersecurityconference.org/>
  1. **NICE Annual Conference**
* Danielle let members know the 8th annual NICE Conference and Expo is scheduled for November 7-8, 2017 in Dayton, OH.
* This year’s theme, “Challenging the Status Quo: Building a Robust and Sustainable Cybersecurity Ecosystem,” was chosen to inspire presentations that aim to shape the way in which the nation identifies, educates, trains and builds a 21st century cutting-edge Cybersecurity Ecosystem.
* The conference will feature 3 tracks:
  + - 1. Developing Cybersecurity Talent through Education and Training
      2. Nurturing Cybersecurity Communities through Academia, Industry, and Government Collaboration
      3. Professional Development
* The Call for Proposals submission deadline is May 31, 2017. Decisions will be made in early June with a full schedule and conference sign up ready in July.
* Find out more here: <https://www.fbcinc.com/e/nice/default.aspx>
  1. **NICE Challenge Project**
* James Ashley, Project Manager, provided an update on the NICE Challenge Project. New content released includes a new threat sandbox. Users can play with real world vulnerabilities.
* A newsletter will go out later today. Subscription requests are located on our [website](https://www.nice-challenge.com).
* Platform development continues nearing release of a ticketing system.
* This project will be visible at several conferences over the summer.

1. **New Business** – David Tobey spoke about the National CyberWatch Curriculum Standards

* This is a new initiative set up to change the scale of cybersecurity education. There is a need to start thinking at the micro level. A new type of online experience is under development where analysis is on curriculum and breaking it apart in order to accelerate and enhance the cybersecurity experience.
* The curriculum begins with a foundation series and aligns with the NICE framework and integrates IT infrastructure into career pathways.
* It is anticipated there will be development in topic areas and delivery capacities.
* Cybersecurity is continuously updated. Setting up topic area working groups will begin by identifying a mapping.
* The purpose is to move individual learners from a basic understanding to a master level. To also integrate a tutorial lab to augment skills and finally move to internships and apprenticeships in order to raise to mastery level.
* Education begins when someone does not understand something or misconceives it. There is a need to determine what conditions and situations will work the best.
* Integrate with lab and various tools already in the marketplace.
* Stacked credentials expand knowledge and save time.
* David is asking for instructional designers, practitioners, etc. who can participate in working groups beginning in the next few weeks and for years to come.
* NICEWG participants who would like to participate include Laurin Buchanan, Stephen Miller and Diane Groth.
* See presentation and find out more here: <https://www.nationalcyberwatch.org/programs-resources/curriculum/>

1. **Summary of Action Items**

* Meeting minutes and presentations will be shared with the group once available.
* The NICE Conference call for proposals deadline is May 31, 2017.
* The NICE K-12 Conference call for proposals deadline is May 31, 2017.
* As a reminder, the Program Office is always looking for topics, help, ideas, and suggestions on the standing items portion of the agenda each month. Contact the Program Office with recommendations. [nist.nice@nist.gov](mailto:nist.nice@nist.gov)

1. **Next Meeting Reminder**

* The next NICEWG meeting is June 28, 2017