**NICE Working Group**

**July 16th Meeting Notes**

**Welcome Remarks (Jane Snowdon)**

**Membership Roll Call**

Organizations represented:

|  |  |
| --- | --- |
| * Cal Poly Pomona
 | * iQ4
 |
| * Commonwealth of Virginia
 | * ISACA
 |
| * DHS
 | * JPMorgan Chase
 |
| * Federal Communications Commission
 | * NIST
 |
| * Harvard University
 | * Northrop Grumman Corporation
 |
| * IBM
 | * University of TX at San Antonio
 |
|  | * University of Washington, Takoma
 |

**Government Update (Bill Newhouse)**

Feedback to Draft Nice Strategic Plan:

Steve Chan made a comment for recommendation on the Vision Statement.

 Vision: A cyberinfrastructure and digital economy that is powered by secure and resilient digital technologies, supported by a skilled ~~cybersecurity~~ workforce, and consumed by cyber aware citizens.

Montana Williams made a comment for recommendation on the Mission Statement.

 Mission: To foster and promote an ecosystem of cybersecurity education, training, and workforce development that effectively secures cybersecurity resiliency.

**Industry Update (Jane)**

* 1. NYU – Women’s Security Symposium, July 30, 2015
		+ A symposium to help expand the career pathway and pipeline for women in security.
		+ <https://cybersymposium.engineering.nyu.edu/>
	2. Penn State Security Conference, October 14-15, 2015
		+ Call for Proposals due July 31, 2015
		+ <http://securityconference.psu.edu/>

Jane mentioned that in the coming NICE WG monthly meetings, there is expected to be discussions around developing policy recommendations as a possible outcome of the work group.

 For example: OPM uses SSN as a unique citizen / employee identifier. A stolen SSN can be used to open a bank account or receive benefits that an individual is not entitled to, etc. Recommend that OPM use a unique personal identifier that is different from a SSN.

 The earlier breach at the VA (stolen laptop which led to an e-benefits platform with 1 central repository) co-joined with the OPM hack provides information to an adversary on active and inactive DoD and other government employees and contractors.

 The Anthem attack has similarities with the OPM attack.

 Recommend internal training within the government for massive context awareness. For example, conduct a phishing simulation as a training exercise. Large corporations, such as IBM and Northrop Grumman, have deployed cyber and phishing simulation training to their employees and are seeing effective results.

 Recommend updating security controls so that the letters OPM sends to individuals with comprised information do not look like a phishing attack.

**Academic Update (No Report)**

**Feedback on C-Cubed Voluntary Program Webinar: “Cybersecurity for Academia” (Christopher Duvall)**

Chis provided an overview of the C-Cubed Voluntary Program. The program recently conducted a Cybersecurity for Academia webinar that was focused on implementing the NIST Cybersecurity Framework in Academia.

The C-Cubed Voluntary Program is closely related to the Protected Critical Infrastructure Information (PCII) Program. The PCII Program is one of the tools that the C-Cubed Program uses as a tool in their toolkit.

Up next with the C-Cubed Voluntary program:

* Small/Medium sized business roadshow
* Partner Program – the C-Cubed Voluntary Program is looking for advocates for implementing the NIST Cybersecurity Framework
* Webinars. The August webinar is scheduled to be a “tools deep dive” this session will be a walkthrough on the C-Cubed toolkit.
* September Event: for small/medium sized businesses, Academia, and State, Local, Tribal, and Territorial organizations.

**New Business: Save the Date – NICE Conference (Bill)**

The NICE Conference will be held in San Diego, CA on November 3-4, 2015. The call for proposals is open for the NICE Conference. Submissions will be accepted until September 9. Please see the following link for more information: <http://csrc.nist.gov/nice/events/nice2015/index.html>

**New Business: NCSAM (Princess Young)**

The Stop.Think.Connect. Campaign is DHS’s National Campaign for cybersecurity awareness. As part of DHS’s awareness programs, the National Cybersecurity Awareness Month is held every year in October. Princess described the weekly themes and descriptions for National Cyber Security Awareness Month 2015. They are as follows:

* General Cybersecurity Awareness
* Creating a Culture of Cybersecurity at Work
* Connected Communities
* Evolving Digital Life
* Building the Next Generation of Cyber Professionals

If there are any events you plan to have that you need support with, please let DHS know via email at stopthinkconnect@dhs.gov. DHS can provide speakers, material s, etc. For more information please visit <http://www.dhs.gov/stopthinkconnect>

**Updates by Subgroup Leaders**

K-12 (No Report):

Collegiate (Morgan Zantua):

No update

Competitions (Dan Manson):

The Cybersecurity Competitions Federation (CCF) Workshop will be held August 25-26, 2015 in Pomona, CA.

The CyberFed Show’s 23rd episode was just posted. More information as well as links to the CyberFed show episodes can be found at <http://cyberfed.org/>

Dan will be attending BlackHat and DefCon. If anyone would like to meet with Dan, please contact him. Dan will also be conducting interviews for the CyberFed Show at these events.

Please contact Dan if anyone is interested in the competitions subgroup.

Technical Training and Certifications (Montana Williams):

ISACA will be meeting with the DoD to discuss how to accredit and validate performance based certifications and how certifications measure functional roles from the NICE Workforce Framework.

Workforce Planning (No Report):

Workforce Framework (Frank Cicio):

iQ4 has launched the Cybersecurity Workforce Alliance (CWA) with The City University of New York and the Securities Industry and Financial Markets Association. This Alliance helps define the roles that industry is looking for and defines courses aligned to those roles.

iQ4 is working with PESC in helping to provide a way to formally show hands-on/project experience by incorporating it into transcripts.

Frank also mentioned that a modification has been made to the No Child Left Behind Bill to include an attachment on cybersecurity. <http://thehill.com/policy/cybersecurity/248229-no-child-left-behind-now-mandates-cyber-education-report>