Report on the International Workshop on Cybersecurity Education and Workforce Development Capacity Building

Danielle Santos
National Initiative for Cybersecurity Education
National Institute of Standards and Technology

Marian Merritt
National Initiative for Cybersecurity Education
National Institute of Standards and Technology

Professor Philip Lark
Program on Cyber Security
George C. Marshall European Center for Security Studies

November 12, 2019
nist.gov/nice

Table of Contents

Overview

On September 9-13, 2019, in Garmisch-Partenkirchen, Germany, the International Workshop on Cybersecurity Education and Workforce Development Capacity Building brought together 38 participants from 20 countries around the globe to expand on existing international strategies and policies and enhance partnerships and collaboration. The workshop was led by:

- The George C. Marshall European Center (GCMC) for Security Studies Program on Cyber Security Studies (PCSS),
- The US Department of State (DoS), and
- The National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST) in the US Department of Commerce.

The workshop brought together a mix of legal advisers, human resource managers, cyber strategy planners, and policy makers from a variety of organizations that oversee national security including Ministries of Foreign Affairs, Defense and Justice, Education and Communications Commissions, and national cybersecurity agencies. Countries represented included: Australia, Bangladesh, Botswana, Brazil, Georgia, Japan, Jordan, Kenya, Malaysia, New Zealand, Nigeria, North Macedonia, Philippines, Portugal, Singapore, Sri Lanka, Thailand, United Kingdom, United States, Uruguay. Prior to this workshop, NICE did not have established or mature relationships with countries outside of the Five Eyes (Australia, Canada, New Zealand, United Kingdom, and United States). Exposure to the aforementioned countries brought great value to NICE and the extent to which NICE and NIST can collaborate internationally. The workshop was conducted in English and at the unclassified level.

Photo 1 - Workshop participants pose for a picture at the GCMC in Garmisch-Partenkirchen, Germany.

This workshop provided participants with the opportunity to share and learn about strategies, policies, and best practices on developing national-level efforts to educate, train, and build their cybersecurity workforce. The workshop also created the opportunity for countries to share ongoing initiatives, programs, and activities and present ways in which other countries could collaborate with them. The workshop was presented in a variety of formats to encourage

information sharing and group discussion. Plenary presentations provided a spotlight on one to four perspectives at a time while seminar sessions fostered brainstorming and dialogue amongst many countries. The agenda for the workshop is attached.

Workshop Summary

Opening remarks were provided by the GCMC, the workshop host and sponsor, who provided a warm welcome to attendees, described logistics for the week, and provided an overview of the GCMC. The DoS, as workshop co-sponsor, followed by describing their mission in regard to assisting with capacity development. DoS also presented on the United States National Cyber Strategy, which includes a pillar on promoting American prosperity in part by developing a superior cybersecurity workforce. Last, as workshop content coordinators, NICE provided context around the purpose and goals of the workshop and the NICE Strategic Plan objective to collaborate internationally.

The first full day of the workshop focused on National Experiences. Each participating country was asked to prepare a presentation that described their:

1) National strategies, laws, and policies;
2) Organizations that are responsible for cybersecurity workforce development initiatives and an overview of national programs and initiatives;
3) New education, reskilling, and training programs; and
4) Details on how to learn more or how to follow up with appropriate points of contact. Eight countries presented their National Experiences in the plenary while the other countries presented their National Experiences in the seminar breakout groups.

The second full day of the workshop focused on the challenges and opportunities regarding building cybersecurity education and workforce development programs. Three countries presented on their own experiences, then the groups broke into seminars to further discuss and identify top challenges and opportunities relating to their seminar focus area. Groups also examined how challenges can be communicated with leadership in an effective way. To end the day, each seminar group elected one representative to provide an out-brief presentation to the rest of the workshop attendees in the plenary. These presentations summarized their seminar's discussions.

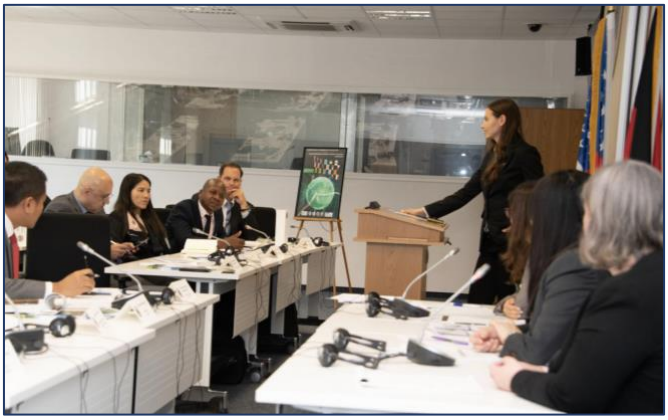

Photo 2 - A panel of presenters take questions during one of the workshop plenary sessions.

The third full day of the workshop focused on developing a national cybersecurity workforce strategy and creating an action plan that can be adapted for future cybersecurity workforce needs. Three morning plenary presentations were followed by seminar breakouts. The group

then enjoyed a lunch break, followed by three afternoon plenary presentations and another round of seminar breakout sessions. To end the day, each seminar group elected one representative to provide an out-brief presentation to the rest of the workshop attendees in the plenary. The workshop closed with remarks provided by the GCMC. Of significance, the attendees were challenged to identify short-, near-, and long-term actions that can be taken.

Seminars

For the seminar breakout sessions, attendees were divided into four groups. Each group focused on a different aspect of cybersecurity education and workforce development over the duration of the workshop. Seminar groups are as follows:

Photo 3- A seminar group meets during a breakout session.

Seminar 1: Forecasting

For the purposes of this workshop, forecasting included mechanisms to measure the current workforce, potential entrants, the gap in supply and demand, and metrics used by government, academia, and industry to describe the cybersecurity workforce.

Table 1 - List of Seminar 1 Participants

Seminar Co-Leads	
Australia	GCMC
Seminar Participants	
Georgia	Jordan
Kenya	Malaysia
Portugal	Thailand
United States	

Seminar 2: Training and Education

For the purposes of this workshop, training and education included classroom, co- and extra-curricular activities, hands-on learning, and on the job training.

Table 2 - List of Seminar 2 Participants

Seminar Co-Leads	
Japan	NICE/United States
Seminar Participants	
Bangladesh	Botswana
Brazil	Georgia
North Macedonia	Organization of American States
Sri Lanka	

Seminar 3: Workforce Planning

For the purposes of this workshop, workforce planning included efforts to identify, recruit, develop, and retain cybersecurity talent.

Table 3 - List of Seminar 3 Participants

Seminar Co-Leads	
NICE/United States	Singapore
Seminar Participants	
Bangladesh	Botswana
Brazil	Georgia
Kenya	North Macedonia
Sri Lanka	Uruguay

Seminar 4: Culture and Climate

For the purposes of this workshop, culture and climate included country-specific circumstances that encourage or hinder the growth of the cybersecurity workforce.

Table 4 - List of Seminar 4 Participants

Seminar Co-Leads	
DoS/United States	United Kingdom
Seminar Participants	
Australia	Malaysia
New Zealand	Nigeria
Philippines	Thailand
United States	

Observations

These observations are a compilation of overall involvement and general activities of the participants to the workshop.

- The Marshall Center's neutral location and excellent facilities greatly enhanced and enabled the participants to focus on the content of the workshop and interact with other participants without distraction.
- Due to the GCMC's strict use of Chatham House Rules, the workshop provided an environment of trust in which all participants felt comfortable sharing their perspectives, especially when it came to discussing challenges and opportunities.
- There was a broad range of countries in attendance. Some had cybersecurity workforce-specific national strategies already developed and several ongoing efforts, while others were still working on a general national cyber strategy and cybersecurity awareness activities.
- Participants agreed that the workshop was helpful in establishing a new network on cybersecurity education and workforce subject matter experts.
- Many of the participants understand the importance of frameworks and national strategies for cybersecurity but are daunted by how to proceed. Many expressed challenges overcoming culture and entrenched bureaucracies.
- Workforce development and recruiting and retention of capable cybersecurity practitioners is a common concern. Participants were optimistic, however, that because their societies include a large number of young people they will be able to develop a robust future cybersecurity workforce.
- Participants lamented that they wished their governments would take cybersecurity workforce strategy development more seriously and wished to work in a more collaborative fashion across their governments.
- Some countries asked for help and sought more information on how NICE works at a practical level.
- Several participants committed to updating draft national cyber strategies to include a workforce component based on the lessons learned from the workshop.
- At the close of the workshop, several participants identified the top "quick win" was that they have become equipped with new ideas to take back to their home country.

Key Findings and Recommendations

These comments should inform future international engagements on cybersecurity education and workforce development.

Challenges and Opportunities

- It is difficult for some countries to obtain funding for capacity building. Discussions took place on how to get leadership to pay attention to capacity building and make it a priority through phishing or tabletop exercises, international rankings, and determining maturity through the Oxford Cybersecurity Model.
- Most countries lack the ability to measure their cybersecurity workforce supply and demand. Where their local workforce boards are unable to meet this challenge, some

countries rely upon data from international consultancies and professional certification bodies.

- The shortage of qualified and experienced cybersecurity teachers and the pay discrepancies between the academic community and the professional sphere creates an ongoing struggle for building academic and professional training programs. Collaborations between universities can help address the shortage of training programs and the ability to keep education updated to current industry needs. One model discussed would be to create partnerships such that universities work together to create a cybersecurity program, each offering their area of expertise (i.e. a university with a strong law school would provide all of the policy courses while a different university or technical school or college would provide the networking and coding courses).
- Instead of retention, one work around can be focusing on knowledge transfer and reskilling. One attendee commented, *"When it comes to government personnel moving to industry for better pay, we won't win over retention, so look at continuity of content, not people".*

Developing a National Cybersecurity Workforce Strategy

- When developing strategy, harmonize with other existing policies and consider where current resources are allocated. Identify the government agency or group of agencies who "own" the strategy. Address issues of authority and autonomy in times of cybersecurity crisis. Practice against threats and vulnerabilities via table-top exercises.
- Cyber hygiene – or general cybersecurity awareness - is often part of cybersecurity strategy programs. Ensure these programs include introductions to cybersecurity careers.
- The adoption of standardized work roles is in its infancy and is recognized as a best practice for aligning all parts of the workforce pipeline (awareness, education, training, etc). Use of the NICE Cybersecurity Workforce Framework internationally is suggested.
- Create national programs for introducing youth to cybersecurity careers. Consider the United Kingdom's Cyber Discovery program as one example or the United State's CyberPatriot competition as another.
- Create programs to incentivize cybersecurity work in the government. Adopt models such as service scholarships (e.g. the US' Scholarship for Service program), advanced training opportunities, national recognition, rotation programs, and higher salary bands.
- Identify or adopt assessment tools for measuring aptitude and ability in youth or job applicants. This should be part of a strategy for building awareness of cybersecurity careers.
- During strategic development, include key stakeholders so that they can have buy-in and are able to make commitments during development so that when it's time for implementation there is better likelihood that they will produce quality results. The training and education seminar developed a list of such key parties. See attachment.

Creating an Action Plan: Adapting Now to the Future

- Public/private activities are best for taking efforts from small pilot projects to fully-implemented programs.
- Consideration for schemes to address diversity should be encouraged: consider low-income students, women, displaced workers, and others who may need training programs to bridge skills from one occupation to another, language skills, and other investment mechanisms.
- Identify methodology for regular reporting of cybersecurity specific labor market supply and demand. Consider CyberSeek.org type of data reporting. Establish key performance indicators and report them publicly.
- Establish defined critical infrastructure sectors and set criteria for regular meetings and information sharing.
- Identify key players and establish a council or regular method for leadership to develop shared best practices and establish ongoing cybersecurity threat sharing, training schemes, and professional development.
- Action plans are best if made at the short-, mid-, and long-term levels. Impacts of cybersecurity education and awareness levels are difficult to measure in the short-term and should be a long-term metric, while increases in personnel trained or staff hired can be measured in the short-term.
- Action plans should be re-visited at regular intervals to ensure efforts are relevant. Potentially disruptive technologies such as artificial intelligence, automation, machine learning, big data, internet of things, outsourced services, and cloud computing that may shift demand and potentially interrupt career pathways should be considered at each planning interval.

Post-Workshop Considerations

A primary objective of this workshop was to discover new ways for collaboration amongst various countries. One such mechanism for continued collaboration is through the annual NICE Conference & Expo. Workshop participants were provided with information about the November 18-20, 2019, NICE Conference & Expo as well as an invitation to participate in the conference. Workshop participants were also particularly encouraged to attend the pre-conference seminar that will focus on "Cybersecurity Education and Workforce Development for International Stakeholders".

While information sharing and discovering ways to collaborate was valuable to all participants, many expressed the desire to have guidance on how to recreate programs and how to build their own countries' efforts. A follow up workshop is recommended to create materials that other countries can use as a roadmap for building their cybersecurity education and workforce ecosystem.

Based on the participant feedback, follow-on engagements will focus on the following themes:

- Workforce development and recruiting and retention of capable cybersecurity practitioners as a common concern.
- Informational-exchange of best practices, to include cybersecurity workforce framework guidance, were frequently cited areas where more information is desired. Industry, academia, non-profit, and government organizations should have a closer cybersecurity cooperation mechanism.
- Educating and informing national senior leaders on the broad spectrum of cyberspace threats and challenges to improve prioritization of cybersecurity workforce development in national strategies.

Attachments

Attachment 1: Agenda for the International Workshop on Cybersecurity Education and Workforce Development Capacity Building

Program in Cyber Security Studies

International Cybersecurity Education and Workforce Development Capacity

September 9-13, 2019
Garmisch-Partenkirchen, Germany

MONDAY, SEPTEMBER 09. Building 109.	
AM	***Arrivals to the Garmisch-Partenkirchen. Hotels. Breakfast is provided at the Hotel.*** ***Seminar Leaders and Co-Leaders meeting at 1000 at George C. Marshall Center.***
1145	***Departure from Hotels to George C. Marshall Center (GCMC) for Registration and Opening Remarks will occur at*** ***1145 from Mercure Hotel*** ***1200 from Hotel Wittelsbacher Hof***
1215-1330	Lunch. Marshall Center Dining Facility (DFAC). Building 263 **At 1330 the Bus will take all participants from the DFAC to Building 109**
1400-1530	• Orientation to the Marshall Center & Workshop Administrative Remarks • Travel Vouchers & Departure Remarks • Individual Photos
1530-1700	• Welcome / Opening Remarks from Department of State (DoS), National Initiative for Cybersecurity Education (NICE) & GCMC
1730-1915	• Icebreaker followed by **Dinner at the GCMC Dining facility.** Building 253. • *Bus Departure to Hotels—1915*
TUESDAY, SEPTEMBER 10. Building 109.	
TIME	SESSION
0745-0800	***0745 pick up at the Mercure Hotel*** ***0800 Pick up at the Wittelsbacher Hotel***
0830-0900	**Plenary Session (Plenary 109, Rm 202)** ***INTRODUCTIONS*** [redacted] ***Program on Cyber Security Studies (PCSS)*** [redacted] ***Department of State (DoS)***

1

0900-1000	**Plenary Session (Plenary 109, Rm 202)** ***Why Are We Here?*** Remarks by Department of State and National Initiative for Cybersecurity Education 0900-0915: [redacted] 0915-0930: [redacted] 0930-1000: Open dialogue with delagates
1000 – 1030	**Official Group Photo** / Coffee Break
1030 - 1130	**Plenary Session (Plenary 109, Rm 202)** **National Experiences Presentations.** **Delegations** 1030-1045: New Zealand, [redacted] 1045-1100: Singapore, [redacted] 1100-1115: Brazil, [redacted] 1115-1130: Portugal, [redacted] **Slide 1**. *Introduction to national strategies, laws and policies in place / under development.* **Slide 2**. *Who and What organization is responsible for cyber workforce development initiatives (design, coordination, implementation) Overview of national cyber security workforce development programs / initiatives.* **Slide 3**. *New education, reskilling and training programs highlighting resources dedicated to implement these cyber workforce development initiatives.* **Slide 4**. *Where additional information can be publicly found (websites) and appropriate points of contact for more information.*
1130-1200	**Plenary Session (Plenary 109, Rm 202)** **Q&A Panel with presenters** **Moderator: GCMC**
1200 - 1330	Lunch. Marshall Center Dining Facility. Building 263 ***Transportation Provided. Bus Departure from Dinning Facility 1320***
1330 - 1430	**Plenary Session (Plenary 109, Rm 202)** **National Experiences Presentations.** **Delegations** 1330-1345: Nigeria, [redacted] 1345-1400: Sri Lanka, [redacted] 1400-1415: Uruguay, [redacted] 1415-1430: Japan, [redacted] **Slide 1**. *Introduction to national strategies, laws and policies in place / under development.*

	Slide 2. *Who and What organization is responsible for cyber workforce development initiatives (design, coordination, implementation) Overview of national cyber security workforce development programs / initiatives.* **Slide 3**. *New education, reskilling and training programs highlighting resources dedicated to implement these cyber workforce development initiatives.* **Slide 4**. *Where additional information can be publicly found (websites) and appropriate points of contact for more information.* ******Remaining Delegations presentations will occur in small seminar groups in the afternoon.** *Australia, Bangladesh, Botswana, Georgia, Jordan, Kenya, Malaysia, North Macedonia, Philippines, Thailand, United Kingdom*
1400-1430	**Q&A Panel with presenters** **Moderator: GCMC**
1500 - 1530	Coffee Break
1530-1645	**Seminar Session** **Remaining Delegations National Experiences Presentations in Small Seminar Groups** *Australia, Bangladesh, Botswana, Georgia, Jordan, Kenya, Malaysia, North Macedonia, Philippines, Thailand, United Kingdom* **Slide 1**. *Introduction to national strategies, laws and policies in place / under development.* **Slide 2**. *Who and What organization is responsible for cyber workforce development initiatives (design, coordination, implementation) Overview of national cyber security workforce development programs / initiatives.* **Slide 3**. *New education, reskilling and training programs highlighting resources dedicated to implement these cyber workforce development initiatives.* **Slide 4**. *Where additional information can be publicly found (websites) and appropriate points of contact for more information.* **Seminar 1 - Rm 206:** [redacted] **Seminar 2 - Rm 202:** [redacted] **Seminar 3 - Rm 103:** [redacted] **Seminar 4 - Rm 104:** [redacted]
1645 - 1700	**Plenary 109: Daily Wrap-Up** ***Bus Departure to Hotels 1700***
1900-2100	***Bavarian Dinner.*** **Restaurant Bräustüberl (Fürstenstraße 23, Garmisch-Partenkirchen)** ***Bus Departure:*** ***1830 from Mercure Hotel*** ***1845 from Hotel Wittelsbacher Hof*** ***Bus will depart form Restaurant at 2110.***

WEDNSDAY, SEPTEMBER 11. Building 109	
TIME	SESSION
0745-0800	***0745 pick up at the Mercure Hotel*** ***0800 Pick up at the Wittelsbacher Hotel***
0830 - 0930	**Plenary Session (Plenary 109, Rm 202)** **Cybersecurity Workforce Challenges & Opportunities** **Delegations** 0830-0850: [redacted] (NICE) 0850-0910: Australia, [redacted] 0910-0930: Portugal, [redacted] Delegations discuss their country's challenges and opportunities in the areas of forecasting, training and education, workforce planning, and culture and climate. ***Participants:*** *take notes to discuss during follow-on Seminar Session.*
0930 - 1000	**Q&A Panel with presenters** **Moderator: GCMC**
1000 – 1030	Coffee Break
1030 - 1200	**Seminar Session** **Discuss and Respond to Challenges and Opportunities** • *How would you define the emerging themes?* • *How do you communicate this issue to leaders?* • *What are the top 4 challenges and opportunities?* • *What are the creative ideas to address the challenges?* • *What are standards and certifications that support the theme?* **Seminar 1 - Rm 206:** [redacted] **Seminar 2 - Rm 202:** [redacted] **Seminar 3 - Rm 103:** [redacted] **Seminar 4 - Rm 104:** [redacted]
1200 - 1330	Lunch. Marshall Center Dining Facility. Building 263 ***Transportation Provided. Bus Departure from Dinning Facility 1320***
1330-1500	**Seminar Session** **Discuss and Respond to Challenges and Opportunities** • *How would you define the emerging themes?* • *How do you communicate this issue to leaders?*

	• *What are the top 4 challenges and opportunities?* • *What are the creative ideas to address the challenges?* • *What are standards and certifications that support the theme?* **Seminar 1 - Rm 206:** [redacted] **Seminar 2 - Rm 202:** [redacted] **Seminar 3 - Rm 103:** [redacted] **Seminar 4 - Rm 104:** [redacted]
1500 – 1530	Coffee Break
1530 – 1630	**Plenary Session (Plenary 109, Rm 202)** **Seminar Discussion Backbrief** • 1 representative per Seminar • No more than (2) slides of content • 15 Minutes per Seminar Presentation
1630-1700	**Q&A Panel with presenters** **Moderator: GCMC**
1700	Daily Wrap-Up ***Bus Departure to Hotels 1700***
THURSDAY, SEPTEMBER 12. Building 109	
TIME	SESSION
0745-0800	***0745 pick up at the Mercure Hotel*** ***0800 Pick up at the Wittelsbacher Hotel***
0830-0930	**Plenary Session (Plenary 109, Rm 202)** **Developing a National Cybersecurity Workforce Strategy** **Delegations** 0830-0850: [redacted] (NICE) 0850-0910: Brazil, [redacted] 0910-0930: United Kingdom [redacted] Delegations will discuss how their country has developed a national strategy for their cybersecurity workforce. • *Who are the "owners" of the national strategy?* • *What role does national and local leadership have in developing it?* • *How does government engage with industry and education?* • *What are the primary objectives or pillars?* • *How often is it updated?* • *What are the key mechanisms to implement the strategy? I.e. legislation*

0930 - 1000	**Q&A Panel with presenters** **Moderator: GCMC**
1000 - 1030	Coffee Break
1030- 1100	**Seminar Session** How are themes identified on Wednesday incorporated into the examples provided in the plenary? **Seminar 1 - Rm 206:** [redacted] **Seminar 2 - Rm 202:** **Seminar 3 - Rm 103:** **Seminar 4 - Rm 104:**
1200 – 1330	Lunch. Marshall Center Dining Facility. Building 263 ***Transportation Provided. Bus Departure from Dinning Facility 1320***
1330 – 1430	**Plenary Session (Plenary 109, Rm 202)** **Creating an Action Plan: Adapting Now to the Future** **Delegations** 1330-1350: [redacted] (NICE) 1350-1410: Singapore, [redacted] 1410-1430: Georgia, [redacted] Delegations will discuss how their country has developed a national strategy for their cybersecurity workforce. • *How is your country identifying gaps in supply/demand?* • *What are plans to increase the pipeline? (for example)* ▪ *Building awareness for careers* ▪ *Standardizing roles and career pathways* ▪ *Creating entry opportunities for underrepresented people* ▪ *Removing barriers to employment* • *What incentives are possible for career entrants, for educators, for employers?* • *How are you taking into consideration the impact of future technologies on the workforce?*
1430 - 1500	**Q&A Panel with presenters** **Moderator: GCMC**
1500 – 1530	Coffee Break
1530- 1615	**Seminar Session** How are themes identified on Wednesday are incorporated into the examples provided in the plenary. **Seminar 1 - Rm 206:** [redacted]

	Seminar 2 - Rm 202: [redacted] **Seminar 3 - Rm 103:** [redacted] **Seminar 4 - Rm 104:**
1615-1640	**Plenary Session (Plenary 109, Rm 202)** **Seminar Back-Briefs (consolidated from "Strategy" and "Future" seminars)** • 1 representative per Seminar • No more than (1) slide of content • 5 Minutes per Seminar Presentation
1640-1700	**Conclusion** ***Bus Departure to Hotels 1700***
FRIDAY, SEPTEMBER 13. Departures	

Attachment 2: Training and Education Seminar List of Key Stakeholders

During strategic development, include key stakeholders so that they can have buy-in and are able to make commitments during development so that when it's time for implementation there is better likelihood that they will produce quality results. Groups to consider bringing in include:

- Professional bodies (ISACA, etc)
- Industry and technical training providers
- Accreditation bodies
- Industry councils (ICT sector)
- Ministries of:
    - Education
    - Tertiary Education
    - Women/Child/Disabled/Youth
    - Tribal
    - Foreign Affairs
    - Finance
    - ICT
- Academia
    - Defense, Intelligence, and Law enforcement academies
    - Polytechnic, trade, and technologic schools
- Public service administrations or entity responsible for civil service professional development
- Intellectual property bodies

Additional groups to include AFTER strategy has been developed

- International organizing bodies
- Trade unions

Attachment 3: NICE Conference & Expo Sample Invite Letter

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-

Dear,

On behalf of the National Initiative for Cybersecurity Education (NICE) group, thank you for your interest in participating in the 2019 NICE Conference and Expo, which will be held November 18, 2019 - November 20, 2019, in Phoenix, AZ.

We would be delighted to have you join us. Personal invitations are not necessary to attend since this conference is an open event to bring together thought leaders from industry, government, academia, and non-profit organizations to address the community's Cybersecurity education, training, and workforce needs. Interested participants will need to pay the registration fee to attend.

The organizers are not able to provide financial support to conference and expo participants. Airfare, ground transportation, hotel, meals, travel insurance, and any other meeting-related expenses are the responsibility of the each meeting participant.

If you need to apply for a temporary non-immigrant visa to attend the conference, you are advised to apply for your visa as soon as possible. All applicants must be able to quality for a visa on their own merits under the requirements of the Immigration and Nationality Act. The organizers cannot intervene with the U.S. State Department or an American embassy in another country on behalf of the any meeting participant. You can submit this letter with your visa application to verify the name, dates, location, and purpose of the meeting.

The organizers are not able to call or generate personal letters to the embassy or consulate on your behalf. Conference and expo registration will be open August 26, 2019 - October 20, 2019. A registration receipt will also be generated for participants.

Additional information on the visa process can be obtained from the U.S. Department of State.

Thank you for your interest and we look forward to your participation.

Sincerely,

Rodney Petersen
National Initiative for Cybersecurity Education (NICE)
Applied Cybersecurity Division

NIST