THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

Division on Engineering and Physical Sciences
Computer Science and Telecommunications Board

500 Fifth Street, NW
Washington, DC 20001
Phone: 202 334 2605
Fax: 202 334 2318
E-mail: cstb@nas.edu
www.cstb.org

Cybersecurity Professionalization Workshop
Discussion Questions

What is the scope of the cybersecurity workforce and the professionalization issue?

- What types of workers have responsibility for cybersecurity?
- Which would you include in the cybersecurity workforce?
- How do you assess the quantity of quality of your cybersecurity workforce?
- What shortcomings or challenges do you see in meeting cybersecurity workforce needs?
- How would you assess the effectiveness of existing certificate, assessment, and other professionalization tools? What if anything is missing?

What are possible forms of professionalization, and how might they help address the challenges you've identified?

- What does professionalization mean to you?
- To what extent has professionalization already been happening, through either formal or informal avenues?
- What can be learned from analogies to other fields? What factors are most useful in selecting these analogues (e.g., high intellectual content, rapid rate of change, high stakes)
- What do you see as emerging tools and approaches, and how might they be helpful?

What are the defining characteristics of the cybersecurity field and workforce, and what are the implications for professionalization?

- What is the rate of the change in the cybersecurity challenge and in the skills and abilities needed to address it?
- What are the implications of the difficulty faced in measuring cybersecurity or the effectiveness of different interventions?
- What different roles and responsibilities that should be included in the cybersecurity workforce?
- What are the implications for the different philosophies/approaches (mission-based, risk-based, compliance-based, pure defense) of different organizations?
- What are the implications of cybersecurity activities being split among those with designed cybersecurity roles and those with operational, policy, or management roles?

What are the costs and benefits of various approaches to professionalization?

- How might various approaches increase or decrease the availability of qualified individuals?
- How do the costs, financial and time, compare to the benefits of various approaches to professionalization?
- To what extent do different approaches improve cybersecurity practice and outcome vs. satisfy bureaucratic or other requirements?
- What benefits or hindrances accrue to different stakeholders -- employers, workers, students, and society as a whole – as a result of different approaches?
- How should we measure the costs and benefits of various approaches to professionalization?

What approaches to professionalization would you recommend, and which would you have concerns about?

- Which ones have you adopted or not adopted and why or why not?
- What tools do you wish you had?