

Professionalizing the Nation's Cybersecurity Workforce?

Criteria for Decision-Making

Committee on Professionalizing the Nation's Cybersecurity Workforce:
Criteria for Future Decision-Making

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

Committee Task

- Committee Statement of Task (*Key components*)
 - To consider the role that professionalization could play in enhancing the capacity and capability of the national cybersecurity workforce
 - To identify criteria that could be used by decision-makers in government and the private sector when considering measures to professionalize the cybersecurity workforce.
- Broader DHS Context (*from NICCS portal*)
 - Is cybersecurity ready to be professionalized across the nation?
 - Which jobs within the cybersecurity field should be professionalized and to what degree?
 - Should the federal government lead this effort single handedly?

**COMMITTEE ON PROFESSIONALIZING THE
NATION'S CYBERSECURITY WORKFORCE:
CRITERIA FOR FUTURE DECISION-MAKING**

DIANA L. BURLEY, George Washington University, *Co-Chair*
SEYMOUR E. GOODMAN, Georgia Institute of Technology, *Co-Chair*
MATT BISHOP, University of California, Davis
MISCHEL L. KWON, Mischel Kwon and Associates, LLC
KEVIN R. MURPHY, Colorado State University
PHILIP M. NECHES, Foundation Ventures, LLC.
CHARLES "CASEY" O'BRIEN, National CyberWatch Center,
Prince George's Community College
RONALD P. SANDERS, Booz Allen Hamilton

Staff

JON EISENBERG, Director, Computer Science and Telecommunications
Board
ENITA A. WILLIAMS, Associate Program Officer (through April 2013)
SHENAE BRADLEY, Senior Program Assistant

Report Reviewers

- Byron Collie, Goldman Sachs Group, Inc.
- Stephen Cooper, Stanford University
- Paul E. Gray, Massachusetts Institute of Technology
- Cynthia Irvine, Naval Postgraduate School
- John D. Johnson, Deere & Company
- Anita Jones, University of Virginia
- Susan Landau, privacyink.org
- Fred Oswald, Rice University
- Michael Papay, Northrup Grumman Corporation
- Franklin S. Reeder, Reeder Group, Inc.
- Eugene Spafford, Purdue University

Report Input

- 3 National Public Workshops
(Washington, DC; San Francisco, CA; San Antonio, TX)
- Additional efforts (NSF CyberCorps PI meeting, others)
- Participants
 - Educational institutions and professional development organizations, professional associations
 - Employers: federal, state, and local government, private sector firms
 - Cybersecurity workers
 - Students

Conclusions

Capacity and Capability

- Conclusion 1

More attention to both the capacity and capability of the U.S. cybersecurity workforce is needed.

- Conclusion 2

Although the need for cybersecurity workers is likely to continue to be high, it is difficult to forecast with certainty the number of workers required or the needed mix of cybersecurity knowledge and skills.

Cybersecurity Work and Workforce

- Conclusion 3

Cybersecurity is a field that encompasses more than one kind of work and more than one occupation or profession. Whether and how to professionalize will vary according to role and context.

- Conclusion 4

Because cybersecurity is not solely a technical endeavor, a wide range of backgrounds and skills will be needed in an effective national cybersecurity workforce.

Professionalization

- Conclusion 5

Professionalization has multiple goals and can occur through multiple mechanisms.

- Conclusion 6

The path toward professionalization of a field can be slow and difficult, and not all portions of a field can or should be professionalized at the same time.

- Conclusion 7

Professionalization has associated costs and benefits that should be weighed when making decisions to undertake professionalization activities.

Criteria and Recommendation

Recommendation

Activities by the federal government and other entities to professionalize a cybersecurity occupation should be undertaken only when the:

- Occupation has well-defined and stable characteristics;
- Observed deficiencies in the occupational workforce could be remedied through professionalization; and
- Benefits outweigh the costs.

Criteria for Decision-Making

- Do the benefits of a given professionalization measure outweigh the potential supply restrictions resulting from the additional barriers to entry?
- Does the potential to provide additional information about a candidate outweigh the risks of false certainty about who is actually best suited for a job?
- Do the benefits of establishing the standards needed for professionalization outweigh the risks of
 - Obsolescence (when the knowledge or skills associated with the standard are out-of-date by the time a standard is agreed on) and
 - Ossification (when the establishment of a standard inhibits further development by workers of their skills and knowledge)?

Applying the Criteria

- Criteria for identifying where professionalization may be appropriate
 - Identify trade-offs that should be considered by those seeking to professionalize (including the U.S. government, other U.S. public and private employers, educational institutions, certification bodies, ...)
 - Illustrate the complex set of costs and benefits associated with professionalization
 - Uncertainties may diminish over time, and long-term benefits may ultimately outweigh short-term costs
- Criteria for undertaking professionalization activities
 - Can be used by decision makers to judge when parts of the cybersecurity field have reached the time where professionalization is warranted

Report available
<http://www.cstb.org>

Question, Comments

Diana L. Burley, Ph.D. *Co-Chair*
dburley@gwu.edu