NISTIR 8287

A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce

Danielle Santos
Sanjay Goel
John Costanzo
Debbie Sagen
Patty Buddelmeyer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8287

National Institute of Standards and Technology
U.S. Department of Commerce

NISTIR 8287

A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce

Danielle Santos
Applied Cybersecurity Division
Information Technology Laboratory

Debbie Sagen
Pikes Peak Community College
Colorado Springs, CO

Sanjay Goel
Dept. of Info. Security & Digital Forensics
University at Albany, SUNY
Albany, NY

Patty Buddelmeyer
Southwestern Ohio Council
for Higher Education
Dayton, OH

John Costanzo
Virginia Cyber Alliance and HRCyber Alliance
Old Dominion University
Norfolk, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8287

February 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8287
32 pages (February 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8287

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-0003
Email: nice.nist@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

In September 2016, the National Initiative for Cybersecurity Education, led by the National Institute of Standards and Technology in the U.S. Department of Commerce, awarded funding for five pilot programs for Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. The document that follows provides a summary of the five pilot programs and outlines a roadmap for building similar programs based on the best practices found and lessons learned.

The roadmap for successful alliances to build the cybersecurity workforce requires four primary components: 1) establishing program goals and metrics, 2) developing strategies and tactics, 3) measuring impact and results, and 4) sustaining the effort. Each section of the roadmap provides specific examples and activities that the pilot programs found to be successful and repeatable in other efforts.

Keywords

alliance; collaboration; cybersecurity; education; partnership; RAMPS; stakeholder; workforce.

Supplemental Content

RAMPS Web Page with additional information on the five projects: https://www.nist.gov/itl/applied-cybersecurity/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps

Acknowledgments

The authors would like to thank Cassie Barlow and Sean Creighton of the Southwestern Ohio Council for Higher Education and Tina Slankas of the Cyber Security Canyon for their contributions to this document. The authors also thank those contributors who reviewed drafts of this document: Marian Merritt, Rodney Petersen, Davina Pruitt-Mentle, Kevin Stine, Shannan Williams, Donna Dodson, Jim St. Pierre, and Jeff Marron.

Table of Contents

1 Introduction 1
1.1 Background 1
1.2 Purpose and Scope of Document 3
2 Key Challenges and Strategies to Address Them 5
2.1 Determining Workforce Needs 5
2.2 Connecting Workforce Supply and Demand 5
2.3 Creating Synergy Amongst Existing Programs 6
2.4 Retaining Talent 6
3 Roadmap 8
3.1 Getting Started 8
3.2 Identifying Stakeholders 9
3.3 Building Relationships 11
3.4 Establishing Program Goals 11
3.4.1 Make a Realistic Plan 12
3.4.2 Start the Documentation Processes 12
3.5 Developing Strategies and Tactics 12
3.5.1 Establish Mechanisms for Collaboration 12
3.5.2 Host Events and Activities 12
3.6 Measuring Impact and Results 14
3.7 Sustaining the Effort 17
4 Conclusions and Other Considerations 18
References 19

List of Appendices

Appendix A— Acronyms 20
Appendix B— Best Practices and Example Activities 21

1 Introduction

The cybersecurity workforce shortfall is well documented. According to CyberSeek.org[1], there were 313 735 open cybersecurity-related positions from September 2017 through August 2018. The 2017 Global Information Security Workforce Study states that 1.8 million more cybersecurity professionals will be needed to accommodate the predicted global shortfall by 2022 [1]. The National Initiative for Cybersecurity Education (NICE) is addressing this critical issue by energizing and promoting a robust network and ecosystem of cybersecurity education, training, and workforce development. Supporting this mission, objective 3.3 of the NICE Strategic Plan emphasizes guiding career development and workforce planning by facilitating state and regional consortia to identify cybersecurity pathways addressing local workforce needs [2].

By fostering regional alliances:

- workforce needs of local business and non-profit organizations are better aligned with the learning objectives of education and training providers conforming to the NICE Cybersecurity Workforce Framework,
- the pipeline of students pursuing cybersecurity careers is enlarged,
- more Americans are upskilled and moved into middle-class jobs in cybersecurity, and
- local economic development to stimulate job growth is supported.

1.1 Background

In September 2016, NICE, led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, awarded funding for five pilot programs for Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. These programs focused on bringing together employers who have cybersecurity skill shortages with educators to focus on developing a skilled workforce to meet industry needs within local or regional economies. Awards were provided to universities, a consortium, and a community college who pre-identified partnerships with at least one of each of the following:

- K-12 school or Local Education Agency
- Institution of higher education or college/university system
- Local employer

Each of the five programs had unique approaches to addressing the cybersecurity workforce needs in their region. These efforts included building interest in and pathways to become a cybersecurity professional. Programs also focused on encouraging more employer engagement in local communities in order to influence education and training providers to develop job-driven

[1] CyberSeek.org is an online tool that provides detailed, actionable data about supply and demand in the U.S. cybersecurity job market.

training that provides the skills that businesses need. Brief descriptions[2] of each program are as follows:

Arizona Statewide Cyber Workforce Consortium
State of Arizona Region; based in Phoenix, Arizona
ArizonaCyber.org

The Arizona Statewide Cyber Workforce Consortium, led by Chicanos Por La Causa and Cyber Security Canyon, developed a unified approach to creating cybersecurity resources from a number of existing efforts. The partnership was used to provide a unity of vision, bridging traditional and non-traditional educational pathways to create cybersecurity talent. It also enabled the alignment of employers' efforts through the Greater Phoenix Chamber of Commerce Foundation. Assistance was provided to help align job descriptions to the NICE Cybersecurity Workforce Framework, review curriculum for greater relevance that adheres to program requirements of the National Security Agency and Department of Homeland Security designated two-year National Centers of Academic Excellence programs, and create job experiences for students interested in learning more about the field of cybersecurity. The partnership connected applicants from traditional and nontraditional backgrounds to employers to provide skilled workers for the growing number of cybersecurity positions in state government and the region's critical infrastructure segments, including manufacturing, health care, and the defense industrial base.

Cincinnati-Dayton Cyber Corridor (Cin-Day Cyber)
Southwestern Ohio Region, including Northern Kentucky; based in Dayton, Ohio
cindaycyber.org
Cin-Day Cyber RAMPS Final Report

Led by the Southwestern Ohio Council for Higher Education (SOCHE), Cin-Day Cyber focused on strengthening cybersecurity education to support the growth of a highly-skilled cybersecurity workforce. Working closely with secondary schools, higher education, industry, and government, Cin-Day Cyber researched local current and future job demand, developed and delivered workshops to build career interest in cybersecurity, created and managed cyber-related internships, and facilitated industry and higher education roundtables to develop partnerships that addressed the challenges of the cybersecurity workforce supply and demand in the Cincinnati-Dayton region.

Cyber Prep Program
Southern Colorado Region; based in Colorado Springs, Colorado
ppcc.edu/cyberprep
Cyber Prep Program RAMPS Final Report

The Cyber Prep Program at Pikes Peak Community College established a formal, sustainable

[2] In-depth program outcomes can be found in each of the programs' final reports. An overview of highlighted activities, sorted by topic area, can be found in Appendix B.

partnership between secondary-school districts, employers, and the college. The program built cybersecurity workforce development pathways to address local workforce needs and supported the development of cybersecurity programs in area high schools and in the college's area vocational program. The program created a summer cybersecurity work experience for high school students and provided opportunities for registered apprenticeships to ensure a sustainable cybersecurity workforce for the future.

It is demonstrated through data collected from each of these programs that regional alliances have a positive effect on educational and workforce pathways. Many examples can be provided to support this, including university and community college articulation agreements that helped save students approximately 50 credit hours or 1.5 years of study, internship partnerships that helped place over 100 students with local employers, and several workshops, trainings, career fairs, camps, and forums held. These activities build bridges between higher education and employers looking for current and future employees in cybersecurity.

Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance
Southeast Virginia Region, including Hampton Roads and Tidewater Regions; based in Norfolk, Virginia
securitybehavior.com/hrcyber
HR Cyber RAMPS Final Report

Old Dominion University's Center for Cybersecurity Education and Research coordinated the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber). HRCyber is a partnership of educational institutions, government agencies, non-profit organizations, and private employers focused on developing educational pathways from high school through community college to four-year institutions and continued professional development, providing a capable and fully trained cybersecurity workforce for the region. The specific goal of supporting local economic development and job growth was achieved by aligning regional educational and skills development offerings to the workforce practices and activities of business and non-profit organizations within the Hampton Roads region.

Partnership to Advance Cybersecurity Education and Training
Capital District and New York City Region; based in Albany, New York
albany.edu/facets
Partnership to Advance Cybersecurity Education and Training Final Report

The Partnership to Advance Cybersecurity Education and Training was led by the State University of New York at Albany. New York's Capital Region has a unique workforce potential, with its range of higher education institutions and Science, Technology, Engineering, and Math (STEM) graduates and a growing advanced technology sector. The project built clear educational paths and increased regional workforce capacity for a range of potential careers in cybersecurity based on industry needs.

1.2 Purpose and Scope of Document

As a result of the outcomes and accomplishments of the RAMPS pilot programs, this document

provides a record of the methods and best practices used and presents a roadmap for communities interested in building similar regional alliances. It describes the essential components of a successful alliance and provides examples of activities that can be accomplished by having such partnerships.

This publication was created for those seeking guidance on how to organize and facilitate regional efforts to enhance cybersecurity education and workforce development. While this document explores some elements for consideration when forming alliances, it is not intended to be a how-to guide that gives specific instructions. NIST believes that this is best left to the local or regional experts who are familiar with the needs of their specific community.