

THE  
UNIVERSITY  
OF RHODE ISLAND

# REAL JOBS RHODE ISLAND CASE STUDY:

## Real Jobs Rhode Island Cybersecurity Partnership

Prepared for:

### Rhode Island Department of Labor and Training

Center General Complex  
1511 Pontiac Avenue,  
Cranston, RI 02920

APRIL 2018 REPORT

**Faculty:**

Shanna Pearson-Merkowitz, *Principal Investigator*  
Skye Leedah  
Aaron Ley

**Student Researchers:**

Bridget Hall  
Kristin Sodhi  
Marissa DeOliveira

URI Social Science Institute for Research,  
Education, and Policy.

The University of Rhode Island  
Social Science Institute for  
Research, Education and Policy  
University of Rhode Island  
Kingston, RI 02881

[uri.edu/ssirep](http://uri.edu/ssirep)

# **Real Jobs Rhode Island Cybersecurity Partnership**

## **Real Jobs Rhode Island (RJRI)**

In 2015, The Rhode Island Department of Labor and Training (DLT) awarded funding to workforce development collaborations throughout the state. Funding was provided through development grants to create sector-based partnerships and create a plan to provide workforce training aimed at sector needs. Implementation funding was then provided for these partnerships to develop training materials and train workers in Rhode Island in targeted industries including healthcare, technology, marine trades, and the arts. Sector partnerships were developed through public private partnerships that included industry, workforce intermediaries, and educational institutions to address the economic needs of the state.

### **I. Sector Need**

The Real Jobs Rhode Island Cybersecurity Partnership (RJRICP), led by the Southeastern New England Defense Industry Alliance (SENEDIA), was formed to heighten awareness of the cybersecurity industry's workforce recruitment needs, communicate those needs to the academic community, and deliver programs that aid small businesses associated with the cybersecurity industry in bringing ideas to market. Specifically, the RJRICP was formed for the following reasons:

- The industry needed to train 400 incumbent employees for new cyber-related certifications within a two-year period and seventy new cybersecurity workers within the year.
- Employment of information security analysts was projected to grow 37 percent over a five-year period.
- Over eighty percent of Rhode Island companies had future plans to hire cybersecurity personnel.

These needs meant that employers were unable to pursue additional opportunities and fill vacant positions due to the lack of skilled employees.

### **II. Grant History**

SENEDIA, a non-profit organization that represents defense industry businesses, initially formed in 2002 in response to base realignment initiatives in Rhode Island. It had already been involved with previous initiatives undertaken by the DLT through the development of internship programs and through the Governor's Workforce Board Partnerships (it formally became a partner with the Governor's Workforce Board in 2010). The organization's past experience working with DLT and the opportunity to fund a proposal that met the industry's workforce needs caused the organization to apply for grant funding to train cybersecurity workers. The primary difference between this grant and past grants was that this one offered an opportunity to develop an expanded training program that allowed SENEDIA to extend internships to more

people than in previous grants.

### **III. Goals and Objectives**

The RJRICEP was developed to increase awareness of the industry's needs by recruiting potential workers, communicating needs to the academic community, and helping small businesses bring new ideas to market. In order to accomplish these objectives, the RJRICEP established five specific goals associated with five specific modules.

1. Increase awareness about the industry's cybersecurity needs and opportunities.
  - The RJRICEP designed a Cybersecurity Awareness Training module to fulfill this goal.
2. Execute a cybersecurity Core Competency Assessment that assists sixty unemployed workers, veterans, and students.
  - The RJRICEP designed a Core Competency Assessment module to fulfill this goal.
3. Execute a specialized Cybersecurity Certification Training program to reach 288 under- or unemployed individuals and deliver them the skills needed to qualify for federal and commercial jobs.
  - The RJRICEP designed a Cybersecurity Certification Training module to fulfill this goal.
4. Expand experiential learning opportunities through a Cybersecurity Internship Program to 24 students, veterans, and nontraditional job seekers.
  - The RJRICEP designed a Cybersecurity Internship Program module to fulfill this goal.
5. Create a council of industry and academic mentors, along with online resources, to help bring mature concepts to the marketplace.
  - The RJRICEP designed a Cybersecurity Ideas and Product to Market Council and Resources module to fulfill this goal.

### **IV. Partnerships**

SENEDIA is a trade organization of companies that, having worked together many times since its foundation in 2002, are affiliated with the defense industry. When SENEDIA learned about the Real Jobs funding opportunities, it applied for and received a Real Jobs planning grant, which was used to convene the RJRICEP. While executing its planning grant, SENEDIA distributed an online survey to the defense, manufacturing, hospitality, finance, and healthcare industries, as well as the Providence, Northern RI, and Newport County Chambers of Commerce to assess their cybersecurity personnel needs. SENEDIA used the results of this study to partner with academic, non-profit, and industry partners so that the industry's needs could be met through the delivery of training programs. Finally, the RJRICEP formed a Steering Committee and an Advisory Committee to act as its governing bodies. The RJRICEP Steering Committee was created under the direction of SENEDIA's Executive Director to oversee the strategic plan for program implementation and outcomes. Partners also nominated individuals to participate on an

Advisory Committee, tasked with providing input and feedback from industry partners not directly involved in the implementation process.

**Table 1: Partnership Members and Responsibilities**

<p>Southeastern New England Defense Industry Alliance</p>	<p>Lead Applicant: Convener of the RJRICP; Director of programs oversaw the implementation of the training modules.</p>
<p>Dell SecureWorks</p>	<p>Committed 80 hours of time from staff experts toward training per year; committing to hire five trained and certified program participants yearly; participate in regular meetings to assist in the implementation of the training plan and assess the needs of the cybersecurity industry.</p>
<p>PURVIS Systems</p>	<p>Committed 20 hours of time from staff experts toward training per year; committed to hiring two trained and certified program participants yearly; participate in regular meetings to assist in the implementation of the training plan and assess the needs of the cybersecurity industry.</p>
<p>Raytheon Company</p>	<p>Committed 50 hours of time from staff experts toward training per year; committed to hiring five trained and certified program participants annually; provide access to conference space; provide data analysis, on-the-job training, and supplies; participate in regular meetings to assist in the implementation of the training plan and assess the needs of the cybersecurity industry.</p>
<p>Rite Solutions</p>	<p>Committed 80 hours from staff experts toward training per year; committed to hire five trained and certified program participants annually; provide access to conference space and laboratory facilities; participate in regular meetings to assist in the implementation of the training plan; and assess the needs of the cybersecurity industry.</p>
<p>SEA Corporation</p>	<p>Committed fifty hours of staff time, ten hours of faculty time and 25 hours from staff experts per year; committed to hire five trained and certified program participants annually; provide access to conference space and laboratory facilities; participate in regular</p>

	meetings to assist in the implementation of the training plan; and assessing the needs of the cybersecurity industry.
Roger Williams University	Provide access to its online Bridge platform to serve as a method of information sharing and connectivity between partnership members; faculty/administration time; actively participate in the Cybersecurity Internship Program.
University of Rhode Island, Brown University, New England Institute of Technology, Bryant University, Johnson and Wales University	Committed faculty/administration time; participate in the Cybersecurity Internship Program.
Maritime Cybersecurity Center	Offer the Cybersecurity Awareness Training module; participate in regular meetings to assist in the implementation of the training plan; assess the needs of the cybersecurity industry.
Community College of Rhode Island	Help design and execute training modules that lead to certifications in relevant cybersecurity fields; lead the Cybersecurity Certification Training module on its Newport campus; participate in regular meetings to assist in the implementation of the training plan; assess the needs of the cybersecurity industry.
LaunchCode	Help develop and implement the Core Competency Assessment module; participate in regular meetings to assist in the implementation of the training plan; help refer candidates to modules; assess the needs of the cybersecurity industry.

## **V. Implementation Activities and Processes**

A variety of strategies were used to launch implementation of the grant. A social media campaign was combined with information sessions at high schools, veterans' fairs, and career outreach fairs to recruit prospective cybersecurity industry candidates. SENEDIA also employs a career outreach coordinator who recruits candidates, sponsors industry-academic roundtables so that universities can meet the staffing needs of the cybersecurity industry, and maintains liaisons at the universities so that prospective interns can learn of internship opportunities. Recruits that are interested in defense industry careers are guided toward an online competency assessment developed by LaunchCode so that trainees are guided into the appropriate program that meets their level of competency. SENEDIA RI member companies pledged to hire at least thirty training program graduates for open positions in their industry, while the Naval Undersea Warfare Center Newport Division committed to hire a minimum of 38 training program graduates.

During implementation, the RJRICEP conducted regular meetings with sub-grantees and partners to assess progress and receive feedback. Program success was measured by surveys of participants and training providers, participant follow-up after completion to measure career trajectory and success, monthly meetings by the Steering Committee, and quarterly meetings by the Advisory Committee.

**Table 2: Training Module Overview**

Name of Module	Training Provided	Duration
Module One: Cybersecurity Awareness Training	Increased awareness about the needs and opportunities connected with the Rhode Island cybersecurity sector. Training was derived from the current National Security Career Awareness program, developed from a Governor’s Workforce Board grant, modified to focus on cybersecurity. Training included awareness training and outreach to Rhode Island cybersecurity careers, the role of cybersecurity in small businesses, and cybersecurity needs in academia.	One hour
Module Two: Core Competency Assessment	Assisted potential workers in identifying the experience, education, information, and training needed for success in a cybersecurity sector career. Delivered LaunchCode’s technical assessments through the application process for Dell SecureWorks. Became an online assessment to gauge the abilities of potential workers for certification training, internship programs, or referral to other industries.	Twenty to Thirty minutes
Module Three: Cybersecurity Certification Training	By targeting under- or unemployed workers, this module sought to increase the number of applicants that have the correct certification to work at a higher level in the cybersecurity sector. This training used CCRI-developed modules aimed at both incumbent workers and under- or unemployed prospective workers. After completion, CCRI evaluated module participants for prior learning experience and, where applicable, connected this experience so that applicants were awarded college credit to be used toward the completion of a certificate or an Associate's Degree program.	Five days
Cybersecurity Internship Program	Expanded experiential opportunities for potential workers to gain insight into, and experience in, the cybersecurity sector. This program was initially developed under the Governor’s Workforce Board training grant funds in 2013. The program allowed students to receive training and experience toward a future career in the cybersecurity industry while still working toward their degree. Internships were offered in the fall, spring, and summer semesters, and selected interns received a \$1,500 stipend (\$1,300 from grant funding and the rest from	Twelve weeks



	the intern's sponsoring company) for their participation.	
Cybersecurity Ideas and Product to Market Council and Resources	Designed to advise companies and students on how to develop ideas into marketable products or services, and launched an online resource center with accessible resources from the Rhode Island and national cybersecurity sectors. This relied on mentors from the cybersecurity industry to form a Council of Industry and Academia Mentors on Cyber IP (Intellectual Property) that helped guide development and connect mentees with mentors and resources.	One to Two hours

## **VI. Achievements**

### Partnerships

#### *Collaboration with CCRI*

Participants at CCRI were placed in jobs before finishing their degrees and their new employers in some cases covered the cost of their tuition. Further, CCRI, which is now seeking NSA certification for its cybersecurity degree, and can now offer cybersecurity training without continuous oversight from SENEDIA.

#### *Open communication*

The RJRICEP kept lines of communication among all partners open at all times and without intermediaries. This openness fostered and maintained a spirit of trust and collaboration within the partnership, and was key to its overall strength.

### Recruitment

#### *Robust and varied recruitment efforts*

The RJRICEP used multiple methods of recruitment to attract quality candidates. It held career outreach fairs, hired and utilized an education outreach coordinator to connect with liaisons at colleges and universities, and established a strong social media presence.

#### *Recruitment through colleges and universities*

The RJRICEP established close connections with colleges and universities to gather recruits. It specifically worked with members of these institutions with knowledge about the cybersecurity industry and its educational subject areas. This allowed the RJRICEP to establish a pipeline of potential recruits who could be guided toward the Cybersecurity Internship Program.

### Trainee Barriers

#### *Lack of technical communication skills*

The RJRICEP found that an unexpected number of participants lacked technical communication skills once they began the training process. The RJRICEP responded by developing and integrating a course into its internship program where participants learned how to write a concise white paper and to orally communicate complex material in under a minute to a superior.

### Training

#### *Success of participants*

Interns worked with one of the business partners to bring the product ideas of the interns to market using the services of the Cybersecurity Ideas and Product to Market Council and Resources module. This helped to further improve the quality of training for interns.

#### *High completion rate of rapid certification training*

Although the RJRICEP initially sought to introduce the Rapid Certification Training to a larger pool of Department of Defense (DOD) workers, it exceeded its goal of certifying twelve workers by certifying thirteen of its fourteen recruits.

### Transition from Training to Employment

#### *High completion rate and job placement rate of cybersecurity internships*

The RJRICEP successfully targeted 28 participants for its internship program despite only having a recruitment goal of 24. Of those 28 participants who enrolled in the program, 26 completed it and five of those completing the program were placed in related employment, exceeding the RJRICEP's goal of placing three employees in training related employment.

#### *Encouraging program completion*

The RJRICEP worked specifically with the participants in the Cybersecurity Internship Program to ensure that interns were completing both their schoolwork and internship requirements. Further, the RJRICEP worked with its partner companies to ensure that interns either received a job offer with the company they interned with or introduced them to the hiring process at other partner companies.

### Other

#### *Expansion of training*

SENEDIA has extended the internship program beyond the field of cybersecurity and has used the DLT "pitch" to begin an internship training program in the area of undersea technology.

**Table 3: Performance Metrics for All Training Programs**

<b>IG-01 Real Jobs RI Cybersecurity Partnership (RJRICP)</b>	<b>Start Date of First Cohort</b>	<b>Proposed End Date for All Cohorts</b>	<b>Target Enrollment</b>	<b>Enrolled</b>	<b>Target Completed</b>	<b>Completed</b>
<b>Recruitment, Training, and Employment</b>						
Cybersecurity Internships - 2016	1/1/16	3/31/17	24	28	24	26
Rapid Certification Training - 2016 (Job Seekers)	1/1/16	12/31/16	6	7	6	6
Rapid Certification Training - 2016 (Incumbents)	1/1/16	12/31/16	6	7	6	7
Direct Job Placements - 2016 (Job Seekers)	1/1/16	12/31/16	0	3	0	3
Undersea Technology Internships - 2016/2017	9/1/16	9/30/17	10	11	10	8
Total Participants placed in related employment- Cybersecurity Internship Program					3	8
<b>Other Objectives</b>						
Awareness Presentation to Potential Future Workers					15	17
Awareness Presentation to Small Businesses					6	6
Total Participants recruited/assessed- Cybersecurity Rapid Certification					60	101

Total Participants Receiving certifications- - Cybersecurity Rapid Certification					TBD	3
Total Participants placed or retained in related employment- Cyber Security Rapid Certification					TBD	8
IP to Market Mentorships					2	2

## **VII. Challenges**

### Partnerships

#### *Finding the time to collaborate*

The RJRICEP found that time was the biggest obstacle to collaboration among industry partners. Many of its partners are small businesses that cannot afford to sacrifice substantial periods of time without it taking away from attending to their own matters. The RJRICEP addressed this challenge by minimizing time commitments required for participation by member partners and finding convenient times to schedule meetings that did not interfere with small business hours.

### Recruitment

#### *Department of Defense security clearance*

Strict requirements are in place for defense industry employment. Recently, the national timeline for approving basic security clearance was extended from taking one month to taking anywhere from six to nine months. As a result, training participants faced a long gap between the time they were interviewed and hired and the date they could start work. Further, participants must be US citizens and must have no criminal record to meet the government's security clearance standards. These requirements limited the number of recruits that could participate in cybersecurity training. However, this issue is being addressed by asking companies that are sponsoring interns to encourage trainees to apply for security clearances when the internship program begins. That way if the company wants to hire the intern as a full time employee at the start of their internship, the intern will either have received the security clearance or will be close to receiving one.

#### *Outreach to veterans*

Veteran outreach proved to be challenging for the RJRICEP given its perception that veterans tend not to attend veterans' fairs. For those veterans participating in the training programs it can be challenging to make accommodations for the part-time jobs that they already hold and for their family-related responsibilities. Yet, the RJRICEP overcame these challenges with veterans by being flexible with internship hours and offering a stipend.

### Trainee Barriers

While RJRICEP discussed no particular achievements in relation to overcoming trainee barriers, its training completion rate was very high.

### Training

RJRICEP discussed no particular achievements in relation to overcoming the training provided. However, in all but one of the training programs RJRICEP trained more individuals than it originally planned for.

### Transition from Training to Employment

RJRICP discussed no particular achievements in relation to transitioning trainees from training to employment. However, it placed more people into employment than it originally aimed to.

### Other

#### *Alterations in industry skill requirements*

When SENEDIA designed the RJRICP's five modules, it did so on the basis of the skills that the DOD had proposed for its employees and contractors. On the basis of financial considerations, DOD scaled back its originally proposed skill requirements needed for employment in the defense industry. This decision occurred after SENEDIA had already written its grant on the basis of the original skill requirements, requiring SENEDIA to modify its plans for grant implementation. The RJRICP worked with its grant advisor to modify the grant, specifically Module Three, which was created around DOD skill requirements. The RJRICP adjusted Module Three from an independent module with its own trainees to a training module provided to interns in the Cybersecurity Internship Program. Interns now received five days of Cybersecurity Bootcamp training and the CCRI-developed evaluation, both of which were valued at roughly \$2000. While the content remained the same, the targeted training audience was adjusted as a result of this modification. The RJRICP also modified how many people it aimed to train due to the DOD skill requirement changes. Module Two increased from a target of 60 participants to 101 participants, while Module Three changed from a target of 288 participants to 36 interns who received the certification training, while Modules Four and Five stayed the same.

## **VIII. Sustainability**

The RJRICP has high expectations for the sustainability of its training program. First, the internship program will most likely be sustainable without DLT funding, especially since the state recently won a four year grant that will deliver \$1,500 stipends to interns (\$1,300 paid by state and \$200 by industry). Additionally, the skills assessment program on the website is sustainable without grant funding as it is run by LaunchCode, though the RJRICP and employers must still absorb the cost of administering the program. The industry-academia roundtables will be sustainable, as they are very popular in the industry and the minimal costs associated with them are covered by in-kind contributions by roundtable member groups. Further, the certification training offered in Module Three that was incorporated into the internship program can be separated from the internship and offered to new recruits and incumbent workers who want to increase their skills on a limited basis in the future if the internship loses state grant funding. Further, the RJRICP is confident that the industry mentorship currently offered by the formal committee will continue informally if the program dissolves because informal mentorship has always been a facet of the industry. SENEDIA plans to facilitate this mentoring by offering professional development classes for former interns, developing a professional network of former interns, and increasing pipeline efforts in state K-12 schools.

Finally, the RJRICEP is hopeful that cybersecurity training in Rhode Island will be sustainable even if the RJRICEP itself dissolves. CCRI, which is now seeking NSA certification for its cybersecurity degree, now can offer cybersecurity training without continuous oversight from SENEDIA. If this development continues, CCRI can offer training similar to the trainings offered by the RJRICEP without RJRICEP assistance or oversight.

## **IX. Lessons Learned**

The following lesson was learned by the RJRICEP in executing its training program:

- Prepare for changes in industry demand and allow for flexibility in training programs to account for the changes.

## **X. Best Practices**

These best practices were utilized by the RJRICEP:

- Provide a weekly stipend to participants in the collegiate internship program to stabilize recruitment to the program and the industry as a whole while also expanding access to training programs for students who need to pay their way through school.
- Provide a standardized competency assessment to program recruits to direct interested potential participants into the right training modules, and identify those who are not suited for a career in the industry prior to their participation in the training.
- Work with a dedicated education outreach coordinator to connect with the industry and the industry pipeline, and facilitate recruitment-

## **XI. Recommendations**

Based on the successes and challenges of the Real Jobs Rhode Island Cybersecurity Partnership, the following recommendation is suggested:

- Allow for flexibility to change implementation plans so that partnerships can respond and adapt to new industry needs.