The Honorable Gina M. Raimondo
Governor of Rhode Island
State House
82 Smith Street
Providence, Rhode Island 02903

December 1, 2015

Dear Governor Raimondo:

Pursuant to Executive Order 15-10, the Rhode Island Commerce Corporation, in partnership with the Rhode Island Cybersecurity Commission submits an action plan outlining steps the state can take to support the growth of a cybersecurity industry and workforce in Rhode Island, leveraging our state's unique assets.

Enhanced cybersecurity skills within the workforce will be required to support job growth across all industries and sectors in Rhode Island, especially in highly technical and STEM related fields. This report stresses the need for Rhode Island to: (1) better leverage and invest in our strong academic ecosystem to build a sustainable cyber-savvy workforce; (2) ensure that existing workforce training, fellowships, and grant programs prioritize cybersecurity slots; and (3) establish a cyber-branding and business development program to market state incentives for businesses and employees to relocate for cybersecurity related jobs.

It is important to note that establishing a sound foundation for information assurance, cyber-hygiene, and statewide operational resiliency are core tenants of a good cyber-economy. State governments can no longer afford to think separately about economic development and cybersecurity, as the two are inextricably linked—one fostering the other. Given that, we ask that you also consider the core recommendations in the October report as key elements to a strong economic development platform for cybersecurity in Rhode Island.

Most importantly, they include: (1) establishing a strategic leadership role for cybersecurity that is integrated into the Homeland Security mission for the state and is directly accountable to you; (2) improving statewide executive branch cyber-hygiene, skills training, risk management, and technology deployment; (3) upgrading the state's existing Cyber Disruption Team to create a more enhanced cybersecurity response, outreach and training capability for Rhode Island stakeholders; (4) expansion of the Rhode Island Fusion Center as a center of excellence to better integrate existing state and federal law enforcement, intelligence, defense, emergency response, and critical infrastructure protection operations; and (5) improving the Rhode Island National Guard's connectivity with U.S. Cyber Command and the 24th Air Force—as enhanced training for our soldiers and airmen will most certainly benefit statewide private and public sector stakeholders.

The Commission offers these action plans to help support the State's efforts to reduce cyber risks, increase operational resiliency, ensure that key state agencies in Rhode Island are appropriately resourced, and create a sustainable platform to further build out our economy. In preparing these reports, we are very appreciative of the assistance provided by Secretary of Commerce Stefan Pryor, State Police Colonel Steven O'Donnell, Rhode Island National Guard Commander Brigadier General Christopher Callahan, Emergency Management Agency Director Peter Gaynor, and their respective staff. The Commission Members, along with the myriad of experts interviewed, also provided exceptional insight and commitment to the task. The recommendations provided will lay the groundwork for a more secure and economically prosperous Rhode Island.

Thank you for your continued stand-out leadership addressing cybersecurity risks as well as cyber-related economic development opportunities for Rhode Island.

Sincerely,

Scott DePasquale
Chairman & CEO, Utilidata
Chairman, Rhode Island Cybersecurity Commission

Growing Rhode Island's Cybersecurity Industry and Workforce: An Action Plan

Report to Governor Gina M. Raimondo

Submitted By:

Rhode Island Commerce Corporation

Rhode Island Cybersecurity Commission

December 1, 2015

Contents

Introduction

The cybersecurity workforce and industry will play an important role in the future of the Rhode Island economy. As the Governor's Executive Order articulated in establishing the Rhode Island Cybersecurity Commission, "the challenges presented by the Information Age also present opportunities for business and workforce development as our economy evolves…[R]egular collaboration among government, private sector, and academic leaders will create a mutually beneficial environment that positions the State to improve its cyber defenses and to capitalize on the opportunity to grow a thriving cybersecurity sector."

This report heeds that charge and identifies a set of policy initiatives that will grow and strengthen the cybersecurity workforce and sector in Rhode Island. These initiatives are built on the same framework other states and cities have used to grow their cybersecurity industries: start by creating a strong pipeline of cybersecurity talent, then marshal public and private resources to grow and attract businesses around that workforce. To inform that approach, this report begins with five case studies of other states and cities that have succeeded in the new cybersecurity economy. Next, the report describes the current landscape of Rhode Island's cyber workforce and demonstrates already-existent talent gaps, areas where employers' demand for qualified cyber workers remains unmet.

This report then makes concrete suggestions for policy levers that can help create a talented pipeline of cyber workers in the near and long terms. It identifies action steps for creating and sustaining strong connections between the state's key academic institutions and cyber industry employers, as well as illustrates the ways in which the state's new business incentives can be deployed to attract and expand cyber employers in Rhode Island. The goal of these recommendations is to establish a steady talent pipeline and a healthy cluster of employers to benefit from it. Fortunately, Rhode Island has already assembled many of the key components of this ecosystem, and so the final section of the report recommends ways in which Rhode Island may better promote itself as a hub for cyber talent and industry innovation. In sum, this report makes the following recommendations:

- **Build a robust cyber workforce beginning at the high school level by leveraging the state's new workforce development programs, including:**
    - Pathways in Technology Early College High Schools (P-TECH) to help create a pipeline of young workers with associate's degrees
    - Wavemaker competitive student loan reimbursement fellowships to attract and retain STEM workers with associate's, bachelor's, and advanced degrees
    - Real Jobs Rhode Island grants to train workers at all levels and match them with employers
- **Prioritize cybersecurity within the state's new economic development programs, including:**
    - Innovation vouchers to encourage collaboration between small/midsize businesses and local research institutions
    - Cluster grants to strengthen clusters of related businesses
    - The Rhode Island Commerce Corporation - Naval Undersea Warfare Center collaboration to encourage the commercialization of NUWC innovations
    - Job and real estate tax credits to incentivize the creation of new jobs and construction/renovation of new business facilities

- **Promote Rhode Island's cybersecurity industry as part of the state's new marketing efforts, and target cybersecurity businesses for attraction to and growth in Rhode Island through the state's expanded business development efforts**
- **Evaluate the potential of cybersecurity to anchor or contribute significantly to efforts to create a Rhode Island innovation hub in partnership with employers, universities, and other public and private sector actors.**

Part 1: Case Studies

1.1: Columbus, Ohio

Over the past five years, Columbus has developed its cybersecurity industry and is now considered by many a national hub. Ohio State University (OSU) has helped to provide a consistent supply of trained employees and the State of Ohio has provided tax incentives and grants focused on technology in the Central Ohio region. The Columbus Collaboratory, an innovative public-private organization, has also played a key role in this development.

Academic Institutions: The Columbus region is home to over fifty colleges and universities with a total enrollment of over 130,000 students. Ohio State, one of the nation's largest universities, created a new interdisciplinary undergraduate major in data analytics that is the first of its kind in order to address the shortage in data analytics professionals. OSU also hosts an annual Cybersecurity Day that features prominent cybersecurity speakers in addition to offering networking opportunities for students. In addition to OSU, Columbus State Community College developed a new cybersecurity training degree program to further increase the number of qualified cybersecurity employees in the region. The program was funded through a $600,000 grant from the National Science Foundation and includes private sector and local high school partners. Objectives include establishing a pre-college model for a high school outreach program where students will start the first two years of a cybersecurity curriculum and a cybersecurity educational workshop to develop high school teachers.

Employers: Columbus has a wide array employers across various industries that utilize employees with IT and cybersecurity skills, including finance and insurance companies JPMorgan Chase and Nationwide Mutual Insurance, retail company L Brands, healthcare provider Cardinal Health, and research and development organization Battelle. In addition to these employers, American Electric Power (AEP), working with the U.S. Department of Energy and Lockheed Martin, created a Cybersecurity Operations Center in Columbus that provides early warnings of potential cyberattacks. Since 2010 the Department of Energy has invested more than $150 million in cybersecurity research, development and commercialization projects in which AEP has been involved.

Public/Private Partnership: The Columbus Collaboratory, founded in 2014, is an organization comprised of seven Central Ohio based companies that is aimed at establishing the area as a data analytics and cybersecurity hub. The Collaboratory is funded by the seven partner companies, each giving $1 million a year for four years, as well as $5 million in technology grants from the Ohio Third Frontier Commission, a state agency that promotes technology based initiatives. The Collaboratory created a central location where member companies, including Battelle and American Electric Power, can work together and develop tools to improve

cybersecurity. In addition to benefiting the member companies, the Collaboratory's initiatives include establishing an advanced and entry-level curriculum, courses and learning opportunities to train students in partnership with universities, as well as recruiting interns to work on projects at member companies. The goal of this program is to encourage companies to grow and expand in Central Ohio by increasing the number of data analytics and cybersecurity experts and professionals in the Columbus area.

Government Support: Columbus has been able to build its cybersecurity industry in large part through tax incentives, in addition to grants through the Ohio Third Frontier. The Ohio Third Frontier was created in 2002 in a commitment to create new technology-based products, companies, industries and jobs. One of the Third Frontier's biggest achievements to date was the $5 million grant to establish the previously discussed Columbus Collaboratory. In 2014, The Ohio Tax Credit Authority approved $81 million in tax incentives to attract Amazon to the region to build a $1.1 billion data center.

1.2: San Antonio, Texas

San Antonio has leveraged its academic institutions' cybersecurity programs, strong military presence, and private sector enterprises to become one of the nation's leading cities for cybersecurity. The selection of San Antonio to house the 24th Air Force in 2009 was a turning point for the city as it significantly increased the cybersecurity workforce and provided job opportunities to students from the nationally recognized University of Texas at San Antonio (UTSA) cybersecurity program. All of this has led the city to title itself "Cyber City U.S.A."

Academic Institutions: San Antonio is home to seven universities offering fifty cyber-degree related programs. UTSA recently became one of forty-four institutions designated as a National Center of Academic Excellence in information assurance/cyber defense by the National Security Agency and Department of Homeland Security and was ranked as the best cybersecurity program in the nation according to a Hewlett-Packard report. Further, the Center for Infrastructure Assurance and Security (CIAS) was established at UTSA in 2001 as part of UTSA's new cybersecurity program. The CIAS delivers cybersecurity events ranging from one-hour lectures to multi-day cybersecurity training classes, exercises, and competitions. The CIAS has consistently been called upon by Congress, with support from DHS and the DoD, to strengthen the nation's cybersecurity preparedness. In addition to UTSA, San Antonio also has other nationally recognized academic institutions focusing on cybersecurity including San Antonio College and Texas A&M – San Antonio.

Employers: San Antonio has a significant cybersecurity presence in both the public and private sectors. One of San Antonio's greatest strengths in terms of cybersecurity is that it is home to the 24th Air Force, which is the Air Force's cyber command and oversees approximately 6,000 personnel in cyber defense. In addition to the 24th Air Force, San Antonio is also home to significant cyber units of the Navy, Army, NSA, FBI, and Department of Homeland Security. The cybersecurity private sector is also strong in San Antonio with over 80 private-sector information security companies in the San Antonio Defense Technology Cluster. The Denim Group, Digital Defense, and GlobalSCAPE are among the notable private sector cybersecurity companies located in San Antonio.

Public/Private Partnership: Created through the San Antonio Chamber of Commerce, the San Antonio Cybersecurity committee is responsible for leading the implementation of the San Antonio Area Cyber Action Plan, which aims to establish and promote cyber education, workforce development, cyber research and development, and collaborations among local cyber government, business and academic entities. The committee is composed of corporate leadership from San Antonio's top cybersecurity companies as well as representatives from state government. In June of 2015, through public and private funding, San Antonio named a cybersecurity director who is charged with promoting the growth of the cybersecurity sector through retaining local business, developing a pipeline of prospects for new business recruitment, supporting local incubators and company startup programs, and coordinating with academic institutions to improve curriculums to align with business hiring needs.

Government Support: UTSA's prominence as a university focusing on cybersecurity was recognized in 2014 when the Department of Homeland Security awarded UTSA a two-year $400,000 grant to develop a DHS Scholars program aimed at building a future workforce for federal and private organizations addressing biological and digital threats. Moreover, the Texas Legislature created Emerging Technology Fund (ETF) in 2005 to provide Texas with an advantage in the research, development, and commercialization of emerging technologies. To date, the state has awarded $173 million to 120 companies and provided an additional $161 million to Texas universities. With specific respect to cyber infrastructure funded by the ETF, the UTSA Institute for Cybersecurity ("ICS") was created in June 2007 through a grant administered through the ETF. The ICS is one of the examples of the ETF's success as it was selected as a five-year, $7.5 million DoD grant recipient in 2008. In 2013, San Antonio approved a tax abatement program that went into effect on January 1, 2015 with the goal to attract, retain and expand specific industries and increase employment and high-wage jobs in the region. Included in the four targeted industries were IT and Cybersecurity.

1.3: San Diego, California

San Diego has made a significant effort over the past several years to establish itself as a cybersecurity hub. A catalyst of this movement has been the San Diego Regional Economic Development Corporation (EDC) which, in 2015, helped found a non-profit organization with several local cybersecurity firms called the Center of Cyber Excellence (CCOE).

Academic Institutions: San Diego is home to two of the leading universities with cyber programs, University of San Diego (USD) and the University of California at San Diego (UCSD). In 2015 USD announced its intention to create a center that would offer graduate degree programs in cybersecurity, as well as address cybersecurity issues. The center will be called the University of San Diego Center for Cyber Security Engineering and Technology and included in the plans are a Master of Science in Cyber Security Engineering, which will be offered through the University's School of Engineering, and an online Master of Science in Cyber Security Information Technology Leadership. UCSD is home to the San Diego Supercomputer Center (SDSC), an organized research unit that is considered a leader in data-intensive computing and cyberinfrastructure. The SDSC offers industry partners, researchers, educators, and students camps and workshops including Educator Professional Development (TeacherTECH), which is a program that aims to provide hands-on and web-based activities and curriculum to K-14 educators, as well as Student Workshops (StudentTECH), which offers classes to middle and high school students.

Employers: San Diego has established itself as a cybersecurity hub due in large part due to having an established commercial market, as well as a substantial federal government market. The United States Navy's Space and Naval Warfare Systems Command (SPAWAR) employs over 3,000 professionals in the cybersecurity field and the Department of Defense recently proposed a five-year cybersecurity budget of more than $23 billion. As for the private sector, there are more than 100 cyber firms that employ over 3,500 private sector employees.

Public/Private Partnership: In 2014, a group of cyber companies with operations in San Diego founded the CCOE to promote alignment and collaboration within the San Diego cyber community. Founding members include Sentek Global, Qualcomm, FICO, Lockton Insurance, and SPAWAR. The CCOE has three main initiatives and accomplishes these through a number of programs. One of CCOE's goals is to create new opportunities for businesses through a program titled Secure San Diego which creates and fosters partnerships and projects among the San Diego cyber industry and the region's towns, municipalities, transportation, and tourism industries. A second goal, to attract and nurture talent/workforce development, works with local universities to assist in filling the demand for a cyber workforce. One of these programs, Link2Cyber, connects students from local universities with job opportunities through events that the CCOE hosts at the universities. Finally, the CCOE fosters cooperation throughout the established cyber community by uniting the network of non-profit organizations supporting cybersecurity startups. Membership fees in the CCOE range from $2,500 to $20,000.

Government Support: In 2012, the National Science Foundation gave a grant of $10 million to a group of colleges including UCSD to study the "human side" of cybercrime. Moreover, cyber companies have taken advantage of the California Competes Tax Credit, established in 2014 as a part of Governor Jerry Brown's economic development initiative. Companies including BAE Systems and iboss Cybersecurity were among companies who were awarded almost $20 million in tax credits.

1.4: Connecticut

Connecticut has not historically been a hub for cybersecurity but the state made headlines this past summer when Governor Dannel Malloy signed legislation that directed the state to research and recommend immediate action on countering cyber threats facing Connecticut residents and businesses. While there is not yet significant data on Connecticut's cyber industry, the state has significant cyber related assets to build upon.

Academic Institutions: The University of Connecticut, in partnership with Comcast, established the Comcast Center of Excellence in Security Innovation (CSI) with the mission of leading research, teaching and workforce development in hardware/software/network security. One of UCONN's main goals with CSI was to attract students focused on cybersecurity to the school to develop and train them through yet-to-be-released certificate and degree programs. CSI also hosts CyberSEED, a two day event that brings together top information security professionals and business leaders to have open discussions about emerging cybersecurity trends and formulate strategies.

Employers: Although Connecticut is not yet a major hub for cybersecurity, the state has had several successful cyber firms. For example, in 2014 SilverSky was acquired by BAE Systems for $200 million in an effort to increase the firm's United States footprint.

Public/Private Partnership: There is currently no a public-private cybersecurity partnership in Connecticut. However, its recently passed cyber legislation indicates a partnership may not be far away. The Labor Department, in conjunction with the Department of Economic and Community Development, is conducting an analysis of the Connecticut cybersecurity sector including identification of potential partners in growing the cybersecurity sector including educational institutions and cybersecurity business trade associations.

Government Support: Connecticut Innovations, the State's quasi-public agency, provided over $4 million in grants and federal loans to over thirty technology and innovation companies through the Connecticut Small Business Innovation Research (SBIR) Acceleration and Commercialization program. Additionally, Queralt, Inc., a cloud-based software firm, received over $1.5 million from the U.S. Department of Homeland Security's cyber security division through SBIR.

Historically, Connecticut has never been considered a leading state in the cybersecurity field but that trend has changed in recent years with the State's recent focus on the industry. In 2014 Connecticut became the first state in the country to release a cybersecurity plan in partnership with the state's utilities to help strengthen defense against possible future threats. According to a study by Burning Glass, between 2010 and 2014 Connecticut saw an increase of 98% in cybersecurity job postings. The Connecticut Technology Council ("CTC"), a statewide association of Connecticut technology companies, has also put their focus in attracting cybersecurity firms to the region. In a response to the cybersecurity plan references above, the CTC focused on the fact that the state has undergraduate institutions with 560 Computer Science majors and would like to work with the universities to incorporate more cybersecurity courses into the curriculum and work with the Government to offer loan forgiveness programs or other incentives to keep these graduates in state.

1.5: Massachusetts

Massachusetts has emerged as a major player in the cybersecurity industry in large part due to the large number of technology professionals that graduate from its many universities. The Boston area is home to colleges and universities with approximately 300,000 students and some of the strongest technology degree programs in the nation. Massachusetts also has a significant concentration of venture capital firms which attract recent graduates to stay and start technology and cybersecurity startups locally.

Academic Institutions: One of the chief characteristics that makes Massachusetts an appealing home to cyber firms is its high concentration of colleges and universities. For example, in 2012 Northeastern University was one of four universities that were designated by the NSA as a National Center of Academic Excellence in Cyber Operations. The NSA works with Northeastern to design curricula that matches the agency's intelligence and infrastructure needs. One of the programs that made Northeastern standout to the NSA was the university's cyber operations program. The concentration is through the College of Computer and Information Science and provides students with a designed curricula to prepare themselves for a career in

cybersecurity. Boston University offers a program similar to Northeastern and gives students the option to complete a specialization in cybersecurity. The program not only provides students with a set curricula but also gives students the opportunity to work with Boston University's Center for Reliable Information Systems and Cybersecurity (RISCS). The mission of RISCS is to promote and coordinate research and education in system reliability and information security by emphasizing a multidisciplinary approach. RISCS hosts seminars and events with industry leaders. Due to RISCS, Boston University was recognized by the NSA as a National Center of Academic Excellence in Information Assurance Education and Research.

Employers: One of the key aspects of Massachusetts cybersecurity market is the number of startup companies that are founded and located in the state. In February of 2015, Kaspersky Lab, one of the world's largest privately owned cybersecurity companies, announced the Security Startup Challenge 2015 that will connect cybersecurity startups with business, cybersecurity and industry experts from around the world to research and develop cybersecurity strategies. Another program, the Cybersecurity Factory, is an eight-week summer program for early-stage security startups that invests $20,000 in each team's company. While Massachusetts is a hub for cybersecurity startups, it is also home to larger, more established cyber firms. Raytheon, with headquarters in Waltham, Massachusetts, is one of the world's largest cybersecurity firms.

Public/Private Partnership: The Advanced Cyber Security Center (ASSC), founded in 2011, is a non-profit consortium that brings together industry, university and government organizations to address the most advanced cyber threats. The ASSC is a coordinated effort between companies across all sectors including defense, financial services, healthcare, legal, technology, biotech, universities and the government. The Massachusetts Technology Collaborative (MTC) awarded $50,000 to help build out the Cyber Security Center through the John Adams Innovation Institute, which is the economic development arm of the MTC.

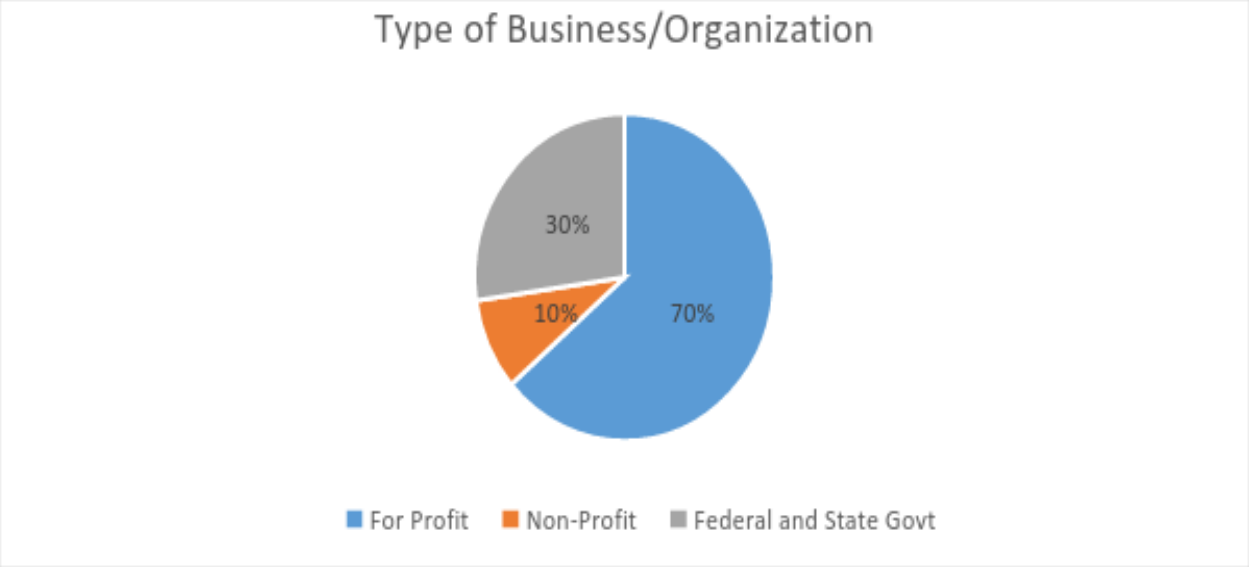
Government Support: Northeastern received a $4.5 million grant administered through the National Science Foundation that is part of the CyberCorps: Scholarship for Service program that provides both undergraduate and graduate students full tuition, fees and a stipend for the final two or three years of their studies. The students then agree to serve for two or three years in information assurance positions in the federal, state or local government or at a federally funded research development center. Additionally, the Massachusetts Technology Collaborative, a state agency, awarded $50,000 to help launch the ACSC described above.

Part 2: Assessing Opportunities and Gaps in Rhode Island's Cyber Workforce

Broadly speaking, it is important that the efforts of state actors to catalyze and grow Rhode Island's cyber industry be informed by the demonstrated needs of the state's industry employers. In this light, the Workforce and Skills Development Subcommittee of the Rhode Island Cybersecurity Commission recently conducted an analysis of the current cyber workforce landscape, as well as an assessment of gaps and opportunities related to growing the state's cybersecurity workforce and economy. This section of the report will summarize the analysis and recommendations coming from the Subcommittee's review.

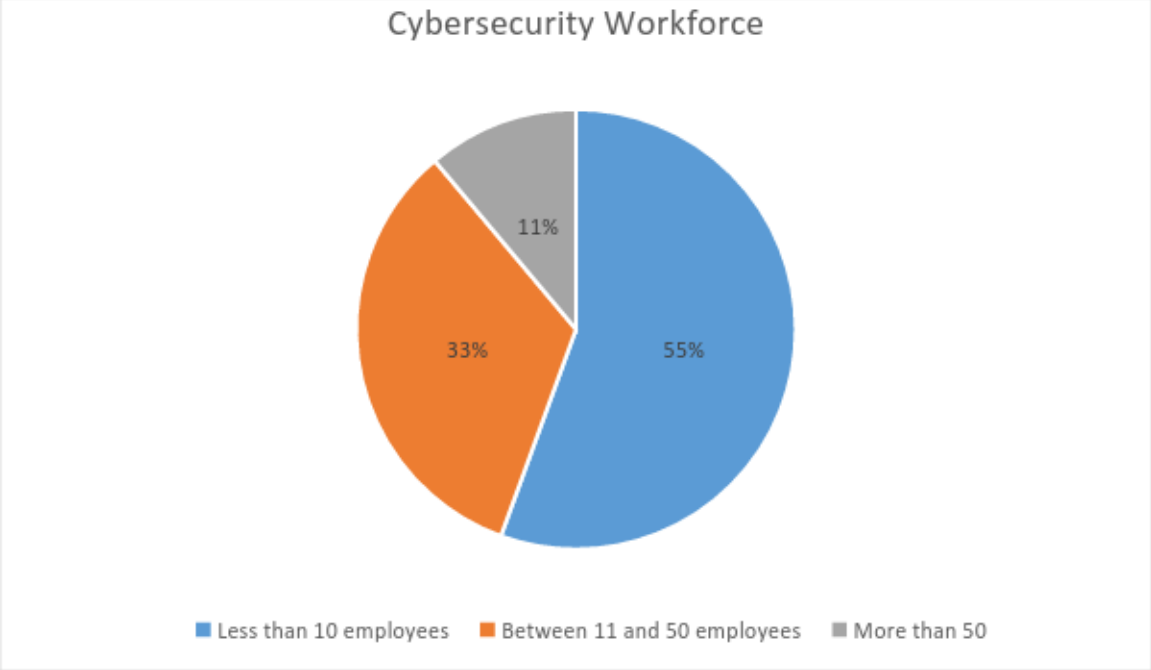
2.1: Survey of Industry Cybersecurity Needs

The Subcommittee surveyed 40 Rhode Island employers to gain a firmer understanding of the current demand for cyber talent in our state. The profile of the respondents is detailed in the charts below.



Half of the participants indicated no existing cybersecurity staff or requirements, though this may be in part due to a lack of understanding or awareness of cybersecurity functions in the context of their particular business and/or a lack of resources to fund.

Of those organizations with identified cybersecurity staff and/or needs, most were small:



Within these firms, the primary responsibilities of employees in cyber-related roles are IT, networks, and information assurance; fewer than 25 percent of cyber employees were identified as having privacy-related responsibilities.

Finally, most of the participating employer reported that most of their cybersecurity workforce is located here in Rhode Island: 60 percent of companies have at least 80 percent of their cyber workforce in-state; 12 percent of companies have between 61 and 80 percent of their cyber workforce in state. Six percent of companies have between 21 and 40 percent of their cyber workforce in the state. 22 percent of companies have less than 20 percent of their cyber workforce located in Rhode Island.

With respect to cyber-related hiring projections, the large majority of organizations surveyed anticipate the need to increase their cybersecurity staffing levels in the next 12 months. 16 percent of firms anticipate no such needs; in contrast, 79 percent of firms anticipate hiring between 1 and 20 cyber staff in the next year – and 5 percent anticipate hiring between 20 and 100 such individuals.

There are clear obstacles, however, to the successful completion of these anticipated hires. Primarily, the surveyed entities identified the lack of qualified candidates with technical certifications as the chief barrier to filling vacant positions; less pressing – but still identified as a challenge – are competition with other companies for the same candidates and the lack of qualified candidates with required experience. Accordingly, job experience and technical certifications are identified by the surveyed employers as the most important criteria in the evaluation of candidates, while experiential training and completion of degreed programs rank somewhat lower on the list

of priority criteria. Among the certifications viewed most favorably by employers, the following are ranked as important or very important: CISSP, Network+, Security+, SSCP, and A+.

2.2: Interviews with Government and Private Sector Actors

As part of the survey of cybersecurity needs in Rhode Island, the Subcommittee performed deep-dive interviews with two large entities in the state: the Naval Undersea Warfare Center, Division Newport (NUWC) and a large company with a Rhode Island presence.

NUWC, with about 3,000 civilian workers in the Newport area, currently reports about 200 government and contractor positions that are designated as part of the Cybersecurity Workforce (CSWF), with a variety of industry standard certifications required for each position including Comptia A+, Comptia Security+, ISC2 CISSP, and additional OS/network environment certificates as required. NUWC expects the need for 300 to 500 more current civilian employees to become CSWF certified in the next one to two years; additionally, NUWC anticipates the hiring of a number of new cybersecurity employees over the next several years to support direct fleet systems requirements. NUWC requirements translate to the requirements of the defense industry that supports them, resulting in a related industry demand for cyber workforce with the required cybersecurity certifications.

The large private company mentioned in the analysis currently reports more than 300 open cybersecurity jobs at the national level, and a willingness to place employees wherever the existing workforce is best equipped to meet the company's labor demand. The company indicated its required cybersecurity workforce could work remotely from any of the company's divisions. The greatest determinant of where the workforce will be located is the availability of a trained cybersecurity labor force from which to hire.

2.3: Current Rhode Island Post-Secondary Cybersecurity Programs

Of the twelve major institutions of higher education in Rhode Island, about half offer cyber-security majors: Johnson and Wales, CCRI, Roger Williams, New England Tech, and Salve Regina. Three offer Master's degrees in cybersecurity, with a handful more offering minors and selected cybersecurity coursework. Nearly all of Rhode Island's colleges and universities offer a Computer Science major, with the exception of RISD and URI.

Cybersecurity Programs at Rhode Island Institutions						
	Offer online degrees?	Computer Science Major	Cyber Security Major	Cyber Security Minor	Cyber Security Classes	Masters in Cyber Security
Brown University	N	Y	N	N	Y	N
University of Rhode Island	Y	N	N	Y	Y	Y (Available Online)
Rhode Island College	N	Y	N	N	Y	N

RI School of Design	**Y**	**N**	**N**	**N**	**N**	**N**
Providence College	**Y**	**Y**	**N**	**N**	**N**	**N**
Johnson and Wales	**Y**	**Y**	**Y**	**Y**	**Y**	**N**
Community College of RI	**Y**	**Y**	**Y (called homeland security)**	**Y**	**Y**	**N**
Roger Williams University	**Y**	**Y**	**Y**	**Y**	**Y**	**Y (Available Online)**
Bryant University	**N**	**Y**	**N**	**N**	**N**	**N**
New England Institute of Technology	**Y**	**Y**	**Y**	**Y**	**Y**	**N**
Salve Regina University	**Y**	**Y**	**Y**	**Y**	**Y**	**Y (Available Online)**
Naval War College	**Y**	**Y**	**N**	**N**	**Y**	**N**

It is clear that the state's academic institutions – taken together – represent a critical component of Rhode Island's cybersecurity present and future, though the extent to which academic cybersecurity curricula are aligned with industry needs remains unclear. Strategic utilization of the state's new employer-driven workforce training initiatives – specifically, Real Jobs RI and P-TECH, described in more detail below – should be a priority for industry and academic partners alike going forward.

2.4: Related Cyber Workforce Development Activities

Two ongoing sets of activities should inform the prospective assessment of the ability of Rhode Island's cyber workforce to meet current and future demand: the Real Jobs RI Cybersecurity Partnership and the cyber-related component of the Apprenticeship RI initiative.

The Real Jobs RI Cybersecurity Partnership arose as a result of Real Jobs RI, the new state job training initiative that convenes industry employers and key stakeholders from government, higher education, and the non-profit sector to build results-oriented, industry-specific job training programs tailored to existing and anticipated employer needs. The following entities make up the Cybersecurity Partnership: the Southeastern New England Defense Industry Alliance (SENEDIA), the primary convening entity, the University of Rhode Island, the Community College of Rhode Island, Roger Williams University, Raytheon, Purvis Systems, Rite Solutions, Sea Corp, Dell SecureWorks, the Maritime Cybersecurity Center, and Opportunity@Work. The partnership will pursue five key objectives: building awareness of industry needs; creation of a cyber competency

assessment tool; internships; short technical certification courses; and expansion of "IP to market mentorship."

At the same time, SENEDIA is also leading the cybersecurity component of the Apprenticeship RI initiative. This will focus on the creation of a non-traditional cybersecurity apprenticeship program, specifically targeting the under- and unemployed, as well as veterans. The effort aims to fill 10 apprenticeships in the first year of its existence; 15 apprenticeships in years two and three; and 18 apprenticeships in years three and four.

Part 3: Building a Robust Cyber Workforce Pipeline

Following the completion of the survey of employer needs and workforce characteristics, the Subcommittee identified three primary gaps in the cyber economy in Rhode Island:

1. Rhode Island industries' cybersecurity needs are greater than the current supply of cyber workers;
2. There is an immediate need to train incumbent workers in cyber-specific disciplines;
3. Rhode Island's small businesses are in clear need of information and training in cybersecurity.

In addition, the Subcommittee identified three clear opportunities to address these gaps:

1. Leveraging other state opportunities presented by Real Jobs RI and Apprenticeship RI;
2. Taking advantage of a strong cybersecurity-related academic ecosystem. A database of cyber-related study programs has been created and will be updated on a yearly basis;
3. Leveraging the tendency of companies to locate their cyber workforce based on the existence of a capable labor supply and not necessarily on the location of the company's headquarters.

Fundamentally, the Subcommittee recommendations for the creation and maintenance of a strong and vibrant cybersecurity workforce ecosystem in Rhode Island – ultimately creating a "cybersecurity hub of excellence" – consist of five key subsidiary points:

1. *Awareness*, including the execution of a marketing/recruitment campaign to attract cyber workers to RI, including creating relationships with national cyber-related headhunters to ensure they are aware of the needs of RI; and the promotion of the National Initiative for Cybersecurity Education (NICE) education framework.
2. *Incentives*, specifically: which new and existing RI economic and workforce development incentives can be applied to the cyber workforce domain;
3. *Learning Environment*, which should foster an ongoing forum for industry and academia to discuss cyber workforce needs and integrating these needs into cyber curricula; in addition, it should ensure an effective system of certifications, internships, and apprenticeships.

4. *Innovation Environment*, including the expansion of IP-to-Market mentorship and support.

Looking forward, the state of Rhode Island is committed to deploying a variety of policy tools to develop the cyber workforce necessary to sustain this sector's continued and expanded presence in the state economy. There are four key areas of focus involved with this effort; below, we address each of them in some detail.

Focus 1: Cyber focus in P-TECH program

The state's new P-TECH initiative represents a key opportunity to grow cyber talent. The P-TECH initiative, which will be implemented in the fall of 2016, is an innovative, proven model that responds to the workforce needs of Rhode Island by creating partnerships between high schools, community colleges, and employers. P-TECH high schools leverage these partnerships, creating a rigorous curriculum that maps directly to current and future job market needs, while creating clear pathways from high school to college and career for students from all academic backgrounds – in six years or less, these students graduate with a high school diploma and a no-cost, two-year associate degree in a growth industry field; from there, they can either move directly into the workforce or on to complete a four-year bachelor's degree.

Rhode Island's employers with cybersecurity workforce needs stand to benefit greatly from this new opportunity. Working with SENEDIA, companies like Raytheon could think creatively about partnering with a high school (potentially on Aquidneck Island) to start developing a pipeline of young, employable workers to meet the cyber demands of today and tomorrow; the opportunity to work with local districts to incorporate the certification needs mentioned above into the 9-14 curriculum stands out as a particularly helpful feature of the P-TECH model. Working with state and local partners to create cyber-specific programming and partnerships within the soon-to-be established P-TECH high schools should be an aim of broader cyber-related workforce development efforts.

Focus 2: Wavemaker Fellowship

A core component of the state's increased efforts to retain and attract talented college graduates is the Wavemaker Fellowship, introduced in the FY 2016 state budget and currently close to full implementation. Recipients of the Fellowship will receive a state tax credit offsetting a significant portion of student loan payments each year for up to four years, provided that they are employed in a STEM field in Rhode Island and commit to staying in the state for the four-year duration of the program.

As the program evolves, the state plans on creating industry- and employer-specific "slots" in the pool of Fellowship applicants – that is, a certain number (or percentage) of each year's Wavemaker Fellows would be placed in a certain company or field. Cybersecurity employers could soon receive this priority status with respect to the Wavemaker Fellowship, increasing the attractiveness of taking up employment in a cyber position in Rhode Island from the perspective of newly-graduated cyber professionals – and from the perspective of the field's employers, increasing the number of motivated applicants locally.

Focus 3: Real Jobs RI

Real Jobs RI, the state's innovative new model for workforce training and development, should factor heavily into the efforts of the cybersecurity industry to meet the demands its employers. The Real Jobs RI model depends centrally on the formation of "industry partnerships" in targeted, high-growth sectors of the state's economy, and their identification of unique, employer-driven workforce training strategies to meet the demands that exist today among the companies forming the partnership. This "demand-side" approach is meant to align the state's training activities with the articulated and identified needs of state employers, and in doing so, increasing the likelihood of the hiring of trained workers upon the conclusion of the training program. As described above, a cyber-industry Real Jobs RI training cluster will grow the capacity of the state to meet the specific needs of Rhode Island's cyber employers at scale, and to create an infrastructure that would allow state job training efforts to respond to the needs of this sector's employers in a dynamic and effective fashion.

Focus 4: Apprenticeship RI

Rhode Island has recently been awarded a federal apprenticeship grant. As part of that grant, SENEDIA is leading the development of a cybersecurity internship program. This will involve developing a set of apprenticeship training standards, which include on-the-job learning, related classroom instruction curriculum, and apprenticeship program operating procedures. After meeting a series of federal requirements, the program will be formally registered with the state and federal labor departments. This well-structured and strategically developed cybersecurity apprenticeship program will wrap around the Real Jobs RI and P-TECH workforce development structures outlined above, ensuring that the industry is reaching as many potential candidates as possible in its recruitment, training, and job-placement efforts.

Part 4: Linking Cyber Employers and Research Institutions

Rhode Island has recently introduced three initiatives that will help connect the state's strong university and federal research and development centers with its key employers, building on the collaboration already fostered by Real Jobs RI and Apprenticeship RI to establish a more robust cybersecurity ecosystem in the state.

The first initiative, the new **Innovation Voucher program**, will assist small and midsize businesses in obtaining technical, R&D, and other assistance from cyber-focused research institutions such as the University of Rhode Island and Naval Undersea Warfare Center. Following application to the Rhode Island Commerce Corporation, companies may receive vouchers worth up to $50,000 to reimburse the participating research institution. Not only will this program help businesses get the help they need, but also it will foster closer relationships between the state's cyber researchers and companies.

The second program, the **Cluster Grant initiative**, will offer competitive grants for companies in the same industry sector (such as cybersecurity) to create or bolster sector organizations that advance the development of the cluster through workforce training programs,

shared equipment and best practices, etc. In tandem with Real Jobs RI sector-based workforce training grants, the Cluster Grant program will incentivize businesses to collaborate to achieve stronger growth.

The third initiative, a **shared NUWC-Commerce Corporation staff person** to be housed at the Rhode Island Commerce Corporation, will help turn cybersecurity and other innovations at the Naval Undersea Warfare Center into businesses and jobs in Rhode Island. Given NUWC's world-class research into undersea communications, sensors, vehicles, and weapons systems, the collaboration holds the potential to result in a significant number of innovative new businesses.

Part 5: Incentivizing Cybersecurity Job Growth

Rhode Island has just implemented three major new tools to encourage job creation, real estate development, and business expansion in key industry sectors such as cybersecurity. These tools are among the most compelling in the Northeast, if not the nation, and will play a major role in growing and attracting cybersecurity businesses in Rhode Island.

The first new tool, the **Qualified Jobs Incentive**, is designed to spur the creation of high-quality jobs. Companies that create substantial numbers of new, above-average-paying jobs are eligible for a refundable, transferable tax credit equal to up to $7,500 per year, for up to 10 years. By providing up to $75,000 per job, the credit is a significant incentive for the creation of new jobs. The per-job credit amount depends on several factors, most notably whether the job is in a promising industry targeted for growth - such as cybersecurity. Jobs in target industries are eligible for the full, $7,500 credit amount - as long as the credit does not exceed the amount of state income tax withholding for those jobs. This provision is designed to ensure that the state receives at least as much in taxes as it pays out in credits.

To give an example of the Qualified Jobs Incentive in action, a new cybersecurity job that pays $75,000 would entail approximately $3,000 in withholding - that would determine the value of the credit. A new cybersecurity job that paid $175,000, by contrast, would entail over $7,500 in withholding - thus, the job would be eligible for the maximum $7,500 per year credit.

The second new tool, the **Rebuild RI tax credit**, is designed to spur the development of new commercial, industrial, and residential facilities, especially facilities that house jobs created by the Qualified Jobs Incentive. Rebuild RI is a refundable, transferable tax credit that can offset up to 30% of project cost, as long as the project can demonstrate a gap in financing or out-of-state competitor that makes the credit pivotal in making a project happen. The Rebuild RI tax credit is limited to the extent of financing gap demonstrated, as well as to 20% of project cost in most industries and 30% of cost in target industries such as cybersecurity. Rebuild RI is payable over the 5 years following completion of the project and issuance of a certificate of occupancy, ensuring public dollars do not flow until a tangible asset is delivered.

To give an example of the Rebuild RI tax credit in action, a new $20 million cybersecurity facility that has secured $15 million in financing could qualify for a $5 million credit (25% of project cost). Once the project is complete and a certificate of occupancy issued, the state would issue $5 million in tax credits over the subsequent 5 years.

Together with the Qualified Jobs Incentive, the Rebuild RI tax credit is able to render many projects effectively rent free for 10 years. The $20 million cybersecurity facility above could qualify for $5 million in Rebuild RI credits and, should it create 250 jobs at an average salary of $90,000, an additional $10 million in Qualified Jobs Incentives. The total $15 million in credits would allow the building to be essentially rent free for the first 10 years - a compelling proposition for current and potential future cybersecurity employers.

The third new tool, the **Anchor Tax Credit**, is designed to encourage existing employers, such as Rhode Island's key cybersecurity employers, to persuade their suppliers, customers, and affiliates to relocate from another state to Rhode Island. The Anchor Tax Credit, therefore, serves as a sort of referral fee, providing a small but meaningful percentage of the value of a resulting new facility to the referring company.

The Anchor Tax Credit may be at play in transactions with the Qualified Jobs Incentive and Rebuild RI, incentivizing a current Rhode Island anchor company to encourage one of its affiliates to move across the border, where the new company also may be eligible for the Qualified Jobs Incentive and Rebuild RI tax credit. **Each of the three tools is discretionary, however: a company must prove it meets the eligibility criteria and offers the state a sufficiently significant and predictable return.**

Part 6: Promoting Rhode Island as a Center of Cybersecurity Excellence

To amplify the effect of new workforce and economic development tools on Rhode Island's cyber industry, the state should act to raise the profile of the industry regionally and nationally. The state will soon complete a comprehensive analysis of the state's economy and identification of target industries with the assistance of the Brookings Institution, Battelle, and Monitor Deloitte. This effort is coalescing around a short list of priority industry areas, and Rhode Island's cybersecurity industry plays an important role here. As part of a broader target industry, cybersecurity will be wrapped into the state's broader efforts to promote these industries, both within and beyond its borders. That effort will entail a concerted public relations and outreach campaign that:

- Promotes the cybersecurity industry within Rhode Island to potential workers, including outreach at high schools aligned with expanded computer science and P-TECH offerings and at colleges aligned with the Wavemaker Fellowship.
- Promotes Rhode Island's cybersecurity industry as part of the Commerce Corporation's business development efforts, including attendance at conferences and trade shows and outreach to prospective cyber businesses for relocation to Rhode Island.
- Promotes Rhode Island's cybersecurity industry as part of the state's new branding and marketing effort, of which economic development is a key part. This effort will include employing paid, earned, and social media to place stories about Rhode Island's innovative economy and compelling business incentives in regional and national media.

Ultimately, the combination of compelling new workforce and economic development initiatives and a concerted communications campaign will help accelerate the growth of Rhode Island's cybersecurity industry and leverage its success to raise the profile of Rhode Island's growing innovation economy more broadly.

Appendix: Additional Information on NICE

NICE, an integral part of the National Institute of Standards and Technology's (NIST) cybersecurity framework, is a national initiative focused on cybersecurity education and workforce development. In support of the need of employers and academia to develop and retain a diverse and qualified workforce, NICE has created a national cybersecurity workforce framework. The framework, which maps to the NIST cybersecurity standards, provides a lexicon for a cybersecurity workforce including related knowledge and skill requirements for defined cyber-related jobs. Rhode Island Emergency Management Agency's (RIEMA**)** Cybersecurity Program is based upon the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity.* The NICE framework should be used as a guide for Rhode Island cyber workforce development efforts.

As part of the U.S. Department of Commerce's "Skills for Business" initiative, NIST has just recently announced that it is funding the development of a visualization tool that will show the demand for and availability of critical cybersecurity jobs across the nation. This will include extensive research and the creation a "heat map" that visualizes the need for, and supply of, cybersecurity workers across the country. Once developed, the map will be updated every 90 days to show job postings grouped into categories mapped to the NICE National Cybersecurity Workforce Framework, using job titles, skills, educational degrees, certifications, experience and other credentials advertised by employers. The NICE Jobs Heat Map will also provide information on the supply of workers with relevant degrees or certifications. The first edition of the jobs heat map is expected to be released in late 2016.