SOUTH CAROLINA

Cyber Ecosystem Strategic Plan

simon
everett
an analytic design firm

FINAL // 30 July 2024

Cover art generated by AI (Bing Image Creator)

Table of Contents

I. Introduction

BACKGROUND

Over the past decade, **South Carolina has made strides** in responding to the rapidly evolving world of cybersecurity[1], which continues to grow in complexity and criticality. In 2015, the state established the South Carolina Department of Administration to provide centralized, shared services—including information technology and cybersecurity—to state agencies. In 2017, Governor Henry McMaster issued an executive order creating the South Carolina Critical Infrastructure Cybersecurity Program to improve cyber threat intelligence and information sharing and improve the overall cybersecurity posture of the state's critical infrastructure. Over this same span, South Carolina became one of the first several states in the US to establish a state Chief Privacy Officer and became the first state to implement cybersecurity requirements for the insurance industry.

More recently, a wide variety of industry, academic, government, and nonprofit stakeholders across South Carolina have been building **an impressive array of cybersecurity programs, resources, and capabilities**. Many SC technical colleges and universities have added cybersecurity courses, certificates, and degrees to their offerings, including seven institutions recognized as Centers of Academic Excellence (CAEs) in Cybersecurity by the National Security Agency and the Department of Homeland Security. Cyber-adjacent workforce development programs like SC Codes and Develop Carolina continue to expand, offering new pathways for South Carolinians to pursue high-paying career opportunities. The South Carolina Council on Competitiveness established CyberSecSC within its SC Tech cluster initiative to help boost the state's competitiveness as a thriving home for cyber industry. And while a statewide team led by the University of South Carolina Beaufort successfully competed for a National Science Foundation cooperative agreement to develop a regional innovation ecosystem focused on cybersecurity applications for maritime, port, and intermodal security, Clemson University led a multi-state team of academic partners to secure a federal grant from the Department of Transportation to establish the National Center for Transportation Cybersecurity and Resiliency.

In light of this widespread cyber development, Governor McMaster's office partnered with the South Carolina Department of Commerce (SC Commerce) and the University of South Carolina in 2021 to conduct an inventory and regional comparative assessment of the state's cybersecurity ecosystem—including cyber companies, workforce, economic impact, and a wide array of enabling assets. Based on the findings and recommendations of that study (the South Carolina Cybersecurity Ecosystem Study, March 2022), the Governor issued an executive order in the fall of 2022 directing SC Commerce to lead a collaborative effort among industry, academia, nonprofits, and government to enhance the competitive standing of South Carolina's cybersecurity ecosystem. In addition to facilitating unity and efficiency of effort, this initiative is designed to result in an intentional landscape of enabling assets that address disparate stakeholder needs—**adding top-down energy and resources to meet the bottom-up successes being realized across the state**.

[1] "Cybersecurity" refers to the safeguarding of (1) electronic information and (2) the devices, applications, and networks that are used to generate, access, transfer, process, or store that information, from (a) damage, to include deletion and manipulation; (b) unauthorized use, including theft; and (c) exploitation, to include holding information "hostage" for ransom. This document uses the terms "cybersecurity" and "cyber" interchangeably.

SC Commerce's role as lead agent for this initiative recognizes **the criticality of cybersecurity to state industry**. South Carolina's leading industry verticals—including automotive (and electric vehicles in particular), aerospace, advanced manufacturing, supply chain management, and port operations—are increasingly reliant on the horizontal enabler of cybersecurity for sustained competitiveness and resilience. Accordingly, a key aim of this cybersecurity ecosystem strategy is to strengthen the state's ability to grow and attract relevant industry assets—namely, cyber companies, investors, and workers.

OBJECTIVES AND INITIATIVES

Guided by the asset inventory and assessment and shaped by the insights and expertise of dozens of stakeholders, this document—South Carolina's first cybersecurity ecosystem strategic plan[2]—presents targeted lines of effort for achieving three overarching objectives. Combined, these three objectives are designed to drive South Carolina's transformation from a cyber-capable state into a cyber-forward state—one ultimately recognized as a national leader in optimizing its full spectrum of cybersecurity ecosystem assets. Each initiative presented within this strategic plan is accompanied by an explanation of how it supports these three objectives:

- **aligning** existing cyber-focused assets and initiatives to improve shared situational awareness, utilize resources more efficiently, and promote unity of effort;
- **augmenting** the state's technical cyber capability and capacity through policies and programs designed to support cyber stakeholders; and
- **attracting** cyber executives, investors, and workers to strengthen and diversify the state's portfolio of enabling assets for cybersecurity.

This strategic initiative will focus on five mutually supportive facets of our cyber ecosystem as shown below, as all efforts are aligned with the overarching goal of **"making cyber accessible"** to our resident industries, agencies, and citizens.

- **EDUCATION & WORKFORCE DEVELOPMENT**: making high-demand, high-earnings careers accessible to South Carolinians, and making a cyber-ready workforce accessible to SC organizations
- **POSTURE & READINESS**: the "doing" of cybersecurity—includes promoting awareness and providing guidance, resources, and support to secure networks, devices, and data
- **INDUSTRY GROWTH:** providing a supportive enabling asset environment to SC cyber companies and positioning SC as an attractive site for relocation or expansion
- **INNOVATION & ENTREPRENEURSHIP:** making cyber technical innovations accessible to SC organizations, and making seed and growth capital accessible to cyber entrepreneurs
- **DEFENSE PARTNERSHIPS:** providing a cyber-ready workforce for US Department of Defense (DoD) missions, making cyber careers accessible to military veterans, and supporting ecosystem collaboration with DoD

[2] This statewide cybersecurity ecosystem strategic plan—which focuses on the collective public, private, academic, and nonprofit landscape—is separate from the cybersecurity plan developed by the South Carolina Law Enforcement Division (SLED) as a prerequisite to qualifying for federal funds via DHS CISA's State and Local Cybersecurity Grant Program. The SLED plan focuses on improving the cyber capacity of South Carolina's (primarily local, per DHS requirement) government agencies, and therefore may be viewed as residing within the "Posture & Readiness" pillar of this overarching ecosystem plan.

For ease of reference and planning, each of the specific initiatives within this strategic plan is primarily assigned to one of the above five "pillars" of our cyber ecosystem. However, each one also will require support from and/or will pay dividends to a secondary pillar. This primary and secondary pillar relevance is shown in the table below, to highlight the intentional "cross-pollination" of priorities and resources that success requires.

	cross-pillar relevance	
	primary	*secondary*
EDUCATION & WORKFORCE DEVELOPMENT		
1. Establish Statewide K-12 Cybersecurity Learning Standards and Supportive Curricula	🟦	🟥
2. Engage Cybersecurity Professionals to Augment K-12 Educator Force	🟦	🟥
3. Develop SC-Specific Cybersecurity Career Pathways	🟦	🟧
4. Promote Early Cybersecurity Awareness and Education	🟦	🟥
5. Facilitate Adoption of Cyber Education Assets at SC Technical Colleges	🟦	🟥
6. Institute a Statewide Cybersecurity Capstone Project Framework	🟦	🟧
POSTURE & READINESS		
7. Fund and Expand the SC CIC Program	🟥	🟧
8. Promote Cybersecurity Readiness Across SC's Industry Supply Chain	🟥	🟧
9. Launch a Centralized Website for South Carolina Cybersecurity Resources	🟥	🟦
INDUSTRY GROWTH		
10. Develop & Market SC's Cyber Ecosystem Brand to Promote Economic Development	🟧	🟩
11. Expand EZone Applicability to Incentivize Cybersecurity Upskilling	🟧	🟦
12. Offset Industry Costs for Security Clearance-Related Assets	🟧	🟪
13. Support Tech Transfer Between NIWC Atlantic and South Carolina Industry	🟧	🟩
INNOVATION & ENTREPRENEURSHIP		
14. Create Joint Appointments for SC Cybersecurity Faculty at SRNL	🟩	🟦
15. Catalyze Investment in SC Cybersecurity Startup and Growth Companies	🟩	🟧
16. Develop a Mentor Network for Cybersecurity Entrepreneurs	🟩	🟧
17. Support SC University-Led, Federally Funded Cyber Innovation Grant Programs	🟩	🟧
DEFENSE PARTNERSHIPS		
18. Increase SC Cyber Employer Participation in DoD Skillbridge Program	🟪	🟦
19. Establish Accelerated Training Program to Support DoD Cyber Missions	🟪	🟦
20. Amplify Aiken / North Augusta Regional Cyber Ecosystem Development Efforts	🟪	🟧

For each initiative listed above, this document includes:

- an explanation of how the item supports the **three primary objectives** (shown on the previous page);
- a narrative **description** of the item's background, intent, vision, and key components;
- a list of **key partners** who should be engaged in (or at least consulted on) implementation;
- a list of **key steps** to be taken towards initial progress; and
- a list of potential **metrics of performance** (MoP) and **metrics of effectiveness** (MoE) that may be considered for measuring success.
    - MoP are used to assess whether implementation activities are proceeding accordingly ("Are we doing the right things?")
    - MoE are used to assess whether the intended results and outcomes are being realized ("Is the work paying off?")

COMPLEMENTARY STATE PLANS

Many of the initiatives in this plan directly support key areas of **South Carolina's Science and Technology (S&T) Plan (June 2022)** and **South Carolina's** (draft) **Unified State Plan for Education and Workforce Development, 2024-2029**. The relevant key areas, goals, and actions from those two plans are indicated for each initiative in the table below, to highlight how these plans are mutually supportive towards South Carolina's continued technological, economic, and social advancement.

	SC S&T plan relevance (area, goal #)		SC Edu/WorkDev plan relevance (area, action #)	
	primary	*secondary*	*primary*	*secondary*
EDUCATION & WORKFORCE DEVELOPMENT				
1. Establish Statewide K-12 Cybersecurity Learning Standards and Supportive Curricula	education 1	education 5	awareness 1	
2. Engage Cybersecurity Professionals to Augment K-12 Educator Force	education 1	education 3	awareness 1	
3. Develop SC-Specific Cybersecurity Career Pathways	education 5	industry 1	skills 3	awareness 1
4. Promote Early Cybersecurity Awareness and Education	education 5		awareness 1	
5. Facilitate Adoption of Cyber Education Assets at SC Technical Colleges	research 1		skills 1	skills 2
6. Institute a Statewide Cybersecurity Capstone Project Framework	industry 1		skills 1	awareness 3
POSTURE & READINESS				
7. Fund and Expand the SC CIC Program	industry 1			
8. Promote Cybersecurity Readiness Across SC's Industry Supply Chain	industry 2	industry 1		
9. Launch a Centralized Website for South Carolina Cybersecurity Resources	industry 1	education 5	awareness 1	awareness 2
INDUSTRY GROWTH				
10. Develop & Market SC's Cyber Ecosystem Brand to Promote Economic Development	industry 1		awareness 1	skills 3
11. Expand EZone Applicability to Incentivize Cybersecurity Upskilling	industry 1		skills 2	awareness 2
12. Offset Industry Costs for Security Clearance-Related Assets	industry 1		skills 3	awareness 2
13. Support Tech Transfer Between NIWC Atlantic and South Carolina Industry	innovation 3	industry 1		
INNOVATION & ENTREPRENEURSHIP				
14. Create Joint Appointments for SC Cybersecurity Faculty at SRNL	research 2	innovation 5		
15. Catalyze Investment in SC Cybersecurity Startup and Growth Companies	innovation 1	innovation 2	skills 3	
16. Develop a Mentor Network for Cybersecurity Entrepreneurs	innovation 3	industry 2	awareness 2	
17. Support SC University-Led, Federally Funded Cyber Innovation Grant Programs	innovation 3	research 3	skills 3	
DEFENSE PARTNERSHIPS				
18. Increase SC Cyber Employer Participation in DoD Skillbridge Program	industry 1		skills 3	awareness 2
19. Establish Accelerated Training Program to Support DoD Cyber Missions	industry 1		skills 1	skills 2
20. Amplify Aiken / North Augusta Regional Cyber Ecosystem Development Efforts	industry 1	innovation 3	awareness 2	

Lastly, many of the initiatives in this strategic plan are supportive towards the **South Carolina Office of Regulatory Services' Digital Equity Plan (February 2024)**. In particular, that plan includes (as one of five overarching goals) a goal of "online privacy and cybersecurity," tied to the objective of every resident of South Carolina being able to safely and securely utilize broadband services. As such, implementers of these two plans should work closely to ensure efficient deployment of resources towards execution of shared activities while managing against duplication of effort.

II. Education & Workforce Development

- **Making cybersecurity education & training accessible to South Carolinians seeking high-paying cybersecurity jobs**
- **Making a cyber-ready workforce accessible to South Carolina cybersecurity companies, state & local agencies, and defense partners**

Many of the challenges manifesting across our cyber ecosystem can be linked to immediate priorities within our cyber education and workforce development landscape. Nearly 6,000 new workers will be needed to meet forecasted cybersecurity labor demand at current growth rates in SC over the next ten years—even before accounting for additional demand generated by initiatives to grow our tech sector. A robust, homegrown cyber workforce is increasingly critical to successfully compete with other states for business attraction and retention, particularly as new norms and technologies enable companies to take a "go where the workers are" approach. Additionally, improving our cyber posture & readiness requires educating residents on computer literacy, security, and science throughout the K-20 landscape, both to raise the public's general level of cyber hygiene and to promote technical innovation that will drive development of advanced products and services.[3] Increased awareness of—and coordination across—local workforce development programs is needed to offer all South Carolinians opportunities to enter the cyber workforce pipeline and to provide our veterans and separating servicemembers with on-ramps to career transition opportunities.

We can only go so far by engaging in a "zero-sum" competition to attract workers from other states and by relying on cyber professionals to mitigate shortcomings in our collective cyber hygiene. We must incubate a cyber-forward citizenry that can strengthen our preventative posture, successfully pursue high-paying career opportunities, and accelerate our economic growth in this increasingly critical technical field.

1. ESTABLISH STATEWIDE K-12 CYBERSECURITY LEARNING STANDARDS AND SUPPORTIVE CURRICULA

- ***Align:*** *Promote uniformity, consistency, and equitable access to cyber educational opportunities and outcomes across the state, irrespective of geographic or socioeconomic factors.*
- ***Augment:*** *Equip future generations with essential cyber skills to ensure a more secure and thriving cyberspace and foster a climate in which businesses can operate securely, residents can engage online with confidence, and the public sector can safeguard critical infrastructure and sensitive data more effectively.*
- ***Attract:*** *Strengthen our pipeline of cyber-forward professionals, positioning the state as an attractive home for industry growth and sustained investment.*

In a rapidly evolving digital landscape, the development of K-12 learning standards and supportive curricula for cybersecurity is a critical undertaking to equip students with the knowledge and skills necessary to navigate the complex world of cyber threats and digital security. With the exponential growth of cyberattacks and data breaches, the need for cyber-literate individuals has never been more pressing. By establishing statewide standards, we will provide a strong foundation in cybersecurity education that spans from

[3] "K-20" refers to the entire educational system, from kindergarten through graduate school.

elementary to high school levels, ensuring that students graduate with the ability to understand, identify, and address potential cyber risks. This comprehensive approach not only prepares them for future educational and professional opportunities but also contributes to building a safer and more resilient cyberspace for our society. But because cyber education is unfamiliar territory for most educators, we must ensure these new standards are accompanied by supportive curricula and materials designed to incorporate cybersecurity concepts into K-12 classrooms. Fortunately, organizations such as CYBER.ORG stand poised to assist our state—at no charge, thanks to federal funding—to develop NICE Framework-aligned standards and materials that can be approved by the SC Department of Education (SCDE) and promoted for use in school districts across South Carolina.[4]

The desired end-state envisions a generation of students who are digitally literate and capable of making informed decisions regarding their online activities and security. These curricula will empower them to protect themselves and their affiliated organizations from cyber threats. Furthermore, they will enhance the cybersecurity workforce pipeline, reducing the skills gap and contributing to the overall security and resilience of our digital infrastructure. The long-term benefits will enhance South Carolina's competitiveness, making the state an increasingly attractive destination for cyber companies seeking access to a highly skilled cyber workforce.

In parallel with the development and implementation of standardized K-12 cybersecurity curricula, it is imperative to recognize the crucial role that teachers play in shaping students' understanding of digital security. As the educational landscape evolves, equipping teachers with the necessary training and resources becomes paramount to ensure the effective delivery of cybersecurity education. Many teachers who may not currently cover cyber-related topics in their lesson plans require specialized training to integrate these concepts seamlessly into their teaching approach. Providing targeted professional development opportunities and support will empower educators to confidently navigate the complexities of cybersecurity, fostering an environment where students can actively engage with and comprehend the principles of digital safety. By investing in the preparation of teachers, we not only enhance their capacity to deliver quality cybersecurity education but also fortify the broader objective of creating a digitally literate generation capable of safeguarding themselves and contributing to the resilience of our interconnected digital society. This commitment to teacher training forms a critical cornerstone in building a comprehensive and effective cybersecurity education ecosystem within K-12 institutions.

By providing K-12 cybersecurity learning standards and supporting curricula approved by the SCDE, we will be laying the foundation for a safer and more secure digital future wherein every individual possesses the knowledge and skills needed to protect themselves and society at large from cyber threats.

[4] The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, developed by the National Institute of Standards and Technology (NIST), facilitates a common understanding of the knowledge, skills, and abilities necessary to perform cybersecurity tasks and functions. It is increasingly viewed as the "gold standard" for ensuring alignment of expectations among educators, students, employers, employees, and policymakers.

Key Partners: South Carolina Department of Education, SC school district leaders, CYBER.ORG

Key Tasks:

- Revise K-12 computer science and computer literacy standards, to specifically include incorporating cybersecurity knowledge, skills, and abilities.
- Engage school district leaders and educators to promote adoption and prioritization of uniform cybersecurity education throughout K-12.
- Collaborate with CYBER.ORG to adopt free, ready-to-implement, and NICE Framework-aligned cybersecurity curricula and materials, to be reviewed and approved by the SCDE.
- Consider incentives for district-wide implementation of SCDE-approved cyber curricula.
- Revise curricula and materials as necessary to align with South Carolina's K-12 standards.
- Ensure materials are accessible to all school districts and emplace centralized mechanisms and resources for continually updating them.

Metrics of Performance:

- *Percentage of Schools Adopting Cybersecurity Curricula*: Measure the percentage of K-12 schools that have adopted the revised curricula.
- *Implementation Timeline Adherence*: Track the adherence of schools and districts to the established timeline for incorporating cybersecurity into the curricula.
- *Number of Educators Trained*: Count the number of educators who have received training on the new cybersecurity curricula.
- *Incentive Program Participation*: Monitor the participation rate of school districts in incentive programs for district-wide implementation.
- *Collaboration with CYBER.ORG*: Evaluate the level of collaboration with CYBER.ORG by assessing the timely adoption of free, NICE Framework-aligned cybersecurity curricula.

Metrics of Effectiveness:

- *Student Cyber Literacy Improvement*: Assess the improvement in students' knowledge and skills in cybersecurity through standardized tests or assessments.
- *District-wide Implementation Impact*: Measure the impact of district-wide implementation on cybersecurity education in terms of student engagement, interest, and understanding.
- *Accessibility and Inclusivity*: Evaluate the accessibility of materials to all school districts, ensuring that no district is left behind.
- *Continuous Curricula Improvement*: Track the frequency and nature of revisions made to the curricula to ensure it stays aligned with evolving standards.
- *Centralized Resource Utilization*: Measure the extent to which centralized mechanisms and resources are utilized by school districts for updating and enhancing cybersecurity materials.

2. Engage Cybersecurity Professionals to Augment K-12 Educator Force

- ***Align:*** *Leverage disparate needs and incentives for cybersecurity companies, professional associations, and educational institutions to create a collaborative framework for addressing the cyber educator gap.*
- ***Augment:*** *Supplement our certified K-12 educator force by engaging cyber professionals who can introduce technical experience and career awareness into the classroom.*
- ***Attract:*** *Strengthen SC's appeal to cyber companies and investors by creatively addressing the cyber skills gap through public-private collaboration.*

The pervasive shortage of cybersecurity professionals across the nation has been extensively documented. Addressing this shortfall requires a comprehensive approach that begins at the elementary school level, fostering an early interest in cybersecurity as both a discipline and a potential career path. Simultaneously, there is a pressing need to enhance the fundamental cyber awareness and hygiene of citizens from a young age. While curricula and programs play a crucial role in laying the groundwork, their effectiveness hinges on the participation of educators and mentors equipped to make cyber concepts accessible and engaging for young learners. These mentors play an essential role in shaping the next generation of cybersecurity experts by instilling knowledge and enthusiasm in the minds of students and bridging the gap between theoretical concepts and practical application.

Accordingly, academic programming for cybersecurity is proliferating across South Carolina, and we are poised to continually grow our future cadre of cyber educators—but we cannot simply wait for that pipeline to bear fruit. Fortunately, there are built-in incentives for private sector individuals and organizations to augment our K-12 educators and accelerate the trajectory of tomorrow's cyber scholars and cyber workforce. For example, cyber workers who hold in-demand cybersecurity certifications (like ISC^2's Certified Information Systems Security Professional, or CISSP) are often required to engage in up to a week's worth of cyber-related education, training, or public engagement each year in order to maintain the validity of their certifications. In addition to possessing the technical and academic cyber experience that some K-12 educators may lack, these professionals can speak to the future cyber career opportunities available to students and help instill an appreciation for baseline cyber skills and awareness. By developing a structured, statewide framework for SC school districts to partner with such organizations, our teachers and students can benefit from the engagement of adjunct cyber educators who can, in turn, use their participation to help satisfy their certification maintenance requirements. Similarly, in today's era of heightened corporate social responsibility, cybersecurity companies often seek opportunities to engage with the public and help improve cyber awareness and hygiene. SC school districts would benefit from a statewide framework they can use to partner with these companies' cyber professionals in adjunct faculty roles—perhaps in the form of a bi-weekly virtual or in-person "cyber hour" that rotates among classes and schools—without having to individually navigate concerns of undue corporate marketing or establish "one-off" partnership agreements.

Key Partners: South Carolina Department of Education, SC school district leaders, SC chapters of cybersecurity professional and technical associations, SC cybersecurity companies

Key Tasks:

- Engage cyber professional associations and companies to explore models for incorporating their members and employees into SC K-12 classrooms as adjunct cyber educators (whether virtually and/or in-person).
- Determine feasible and effective partner engagement models that align with standardized K-12 cyber curricula and learning objectives.
- Decide and codify qualifications, requirements, responsibilities, and authorities for participating organizations and individuals.
- Develop statewide framework to facilitate consistent and streamlined partner agreements between school districts and cyber associations/companies.
- Ensure the provision of state and/or regional resources to manage partner eligibility and requirements and to support school districts in engaging partners.
- Engage partners to develop models, lesson plans, and materials that can facilitate expanded partner engagement.

Metrics of Performance:

- *Number of Cyber Professionals Engaged*: Track the total number of cyber professionals involved in K-12 classrooms as adjunct cyber educators.
- *Diversity of Partner Engagement Models*: Evaluate the diversity and effectiveness of partner engagement models explored with cyber professional associations and companies.
- *Timely Codification of Qualifications*: Measure the time taken to determine, codify, and communicate qualifications, requirements, responsibilities, and authorities for participating organizations and individuals.
- *Number of Partner Agreements Established*: Track the number of partner agreements between school districts and cyber associations/companies established based on the statewide framework.
- *Utilization of State/Regional Resources*: Assess the extent to which state and/or regional resources are utilized to manage partner eligibility, requirements, and to support school districts in engaging partners.

Metrics of Effectiveness:

- *Student Learning Outcomes*: Evaluate the impact on student learning outcomes in cybersecurity by assessing improvements in knowledge and skills.
- *Consistency in Partner Engagement*: Measure the consistency and effectiveness of partner engagement models in aligning with standardized K-12 cyber curricula and learning objectives.
- *Quality of Lesson Plans and Materials*: Assess the quality of lesson plans and materials developed by partners to facilitate expanded engagement.
- *Community Feedback and Satisfaction*: Gather feedback from school districts, educators, and communities regarding the satisfaction and impact of the engagement of cyber professionals.
- *Scalability of Models*: Evaluate the scalability of the models developed, considering the potential for widespread adoption across different school districts.

3. DEVELOP SC-SPECIFIC CYBERSECURITY CAREER PATHWAYS

- ***Align:*** *Demystify the pathways South Carolinians can take to pursue cyber knowledge, skills, and job opportunities within the state.*
- ***Augment:*** *Bolster engagement in South Carolina's robust enabling asset landscape for cyber education and workforce development by showcasing those resources within an easily understandable framework for academic and career progression.*
- ***Attract:*** *Highlight South Carolina's commitment to cyber education and workforce development to increase the influx of talent, minimize the outflow of talent, and substantiate to executives and investors that the state is abundant with resources for sustained cyber workforce growth.*

From technical colleges and research universities to coding camps and apprenticeships, South Carolina boasts a diverse array of resources dedicated to advancing cybersecurity education and fostering career opportunities. However, for students, parents, and mid-career professionals seeking the right path towards a cyber career, it can be challenging to determine which steps to take and where to take them. To enable more South Carolinians to enter the cyber career pipeline, we need to make it easy for aspirants to understand where they are in that journey and identify the in-state programs that can help them advance.

Developing our cyber career pathways will encompass three integral components. First, we will simplify the road maps that aspirants can take to get from where they are to where they want to be. Although a range of federal and non-profit resources have attempted to provide such information in recent years, they often use language designed for curriculum developers, program managers, or human resource professionals—not for students, parents, or career changers. We must design the road map from high school graduate to state government cyber intern or from separating servicemember to federal cyber contractor to be easy to understand and enable a "choose your own adventure" approach to cyber education and career development. Importantly, these pathways must not focus exclusively on purely technical education and training, but also account for the development of "soft skills" necessary to effectively communicate cybersecurity risks and engender the support necessary to address them. Second, we will map these pathways to South Carolina assets—including skills camps, educational institutions, and job opportunities. This asset mapping process will not only make these pathways actionable, but also ensure that all South Carolinians, regardless of their location or socioeconomic background, have equitable access to the wealth of cyber opportunities available within the state. Third, we must communicate these asset-mapped pathways in a clear and concise manner to ensure the information is easily accessible and user-friendly.

The resulting framework and information will reside on a centralized website that encompasses all cybersecurity-related resources available within the state, including educational programs with outcomes ranging from certificates to doctoral degrees; professional development programs; openings for internships, apprenticeships, and employment; specialized opportunities for veterans, and more. Users will be able to explore these in-state resources and visualize pathways tailored to their starting point and desired end state.

Key Partners: South Carolina Department of Employment and Workforce, SC Department of Education, SC Department of Veterans Affairs, SC chapters of cybersecurity non-profit, professional, and technical associations, SC cybersecurity companies

Key Tasks:

- Collect information on cybersecurity certificate and degree programs offered by all institutions of higher education in the state.
- Coordinate with Defense Partnership POCs to ensure incorporation of SkillBridge and similar programs geared towards transitioning servicemembers.
- Collaborate with education and workforce development stakeholders at all levels to create a simplified framework for cybersecurity road maps.
- Establish mechanism for collecting and incorporating information on private sector resources and opportunities.
- Develop a user-friendly online platform and market it to students, parents, and job seekers.
- Establish mechanisms for continual updating of information.

Metrics of Performance:

- *Completion of Information Collection*: Track the completion of collecting information on cybersecurity certificate and degree programs offered by all institutions of higher education in the state.
- *Integration of Defense Partnership Programs*: Measure the successful integration of SkillBridge and similar programs for transitioning service members into the developed cyber career pathways.
- *Stakeholder Collaboration*: Evaluate the level of collaboration with education and workforce development stakeholders at all levels to create a simplified framework for cybersecurity road maps.
- *Incorporation of Private Sector Resources*: Track the establishment and incorporation of information on private sector resources and opportunities into the developed career pathways.
- *User Adoption of Online Platform*: Measure the adoption rate of the user-friendly online platform by students, parents, and job seekers.
- *Continual Information Updating Mechanism*: Assess the effectiveness of the mechanisms established for the continual updating of information on cybersecurity career pathways.

Metrics of Effectiveness:

- *Increased Enrollment in Cybersecurity Programs*: Evaluate the impact on enrollment in cybersecurity certificate and degree programs in the state.
- *Successful Transitions for Service Members*: Measure the success of transitioning service members through SkillBridge and similar programs into cybersecurity career pathways.
- *User Satisfaction with Online Platform*: Gather feedback from users (students, parents, job seekers) to assess satisfaction with the user-friendly online platform.
- *Employment Placement Rates*: Track the employment placement rates of individuals who have followed the developed cybersecurity career pathways.
- *Alignment with Industry Needs*: Assess the alignment of the developed career pathways with the current and future needs of the cybersecurity industry in South Carolina.

4. Promote Early Cybersecurity Awareness and Education

- ***Align:*** *Formalize and expand previous "one-off" activities to promote consistent cybersecurity introduction and awareness for K-12 students across South Carolina.*
- ***Augment:*** *Increase enrollment in South Carolina's cyber education and workforce development pathway programs by strengthening K-12 student cybersecurity awareness and interest.*
- ***Attract:*** *Expand the state's cyber worker pipeline at its source, positioning South Carolina as an assured target for cyber executive and investor attention.*

Addressing the critical shortage of cybersecurity and STEM skills in our workforce requires a proactive approach of instilling technical concepts and career possibilities in young minds beginning as early as K-3. But to make cyber awareness and education engaging and accessible for children, we must deliver knowledge and promote interest through the lens of entertainment, fun, and family activities. While the South Carolina Department of Education has previously implemented such initiatives, our emphasis must now lie in executing these efforts with intentionality and consistency. Developing a core calendar of events shared across state agencies and school districts, featuring at least one central activity or event per month, will be key to fostering early and sustained cyber awareness. These events should be strategically sequenced to complement the standardized cyber curricula learning objectives for each grade level. For instance, computer science-related family movie nights or family coding nights can serve as engaging platforms for learning. By incorporating gamified elements into these events, we can transform education into an enjoyable experience that resonates with children. The importance of marketing these events statewide cannot be overstated, as generating interest and excitement is crucial to their success.

Encouraging schools to augment core cyber events with supplemental activities, such as art competitions or storytelling sessions that incorporate computer science elements, can also help reach new minds and "demystify" cybersecurity. This approach encourages children to view cyber concepts as an integral part of everyday life rather than a technical "other." By involving the whole family in these events, we aim not only to nurture the next generation of cyber workers but also to elevate the general cyber hygiene of our population. Additionally, designing events to appeal to families helps parents better understand the value proposition of cyber careers for their children.

To enhance and expand this initiative, collaboration with the private sector and non-profits is crucial. Partnerships can be formed to secure resources, expertise, and financial support for these events. Cybersecurity companies can offer supplemental workshops or sponsor specific activities, fostering an environment of community engagement. Non-profits may contribute by organizing scholarship opportunities or creating educational materials. Leveraging external support will amplify the impact of these early cyber awareness initiatives, ensuring a comprehensive and sustainable approach to cultivating our cyber workforce of the future.

Key Partners: South Carolina Department of Education (Career and Technical Education), SC school district leaders, School Improvement Councils (SICs) and/or Parent Teacher Organizations (PTOs), SC chapters of cybersecurity professional and technical associations, SC cybersecurity companies, SC Department of Employment and Workforce, the National Security Agency's GenCyber program

Key Tasks:

- Develop a comprehensive calendar of events featuring one central activity or event per month, sequenced to complement standardized cyber learning objectives and designed to engage external partners.
- Engage local SICs/PTOs to determine criteria for activity receptiveness.
- Engage individual schools and districts to augment core events with supplemental activities, providing them with resources to facilitate creative and educational initiatives.
- Forge partnerships with private sector companies and non-profits to enhance these activities' impact by securing additional resources and engagement.
- Promote cross-district collaboration and best practices sharing.

Metrics of Performance:

- *Calendar of Events Completion*: Track the development of the comprehensive calendar of events, featuring one central activity or event per month.
- *Inclusive Participation of State Agencies*: Measure the level of participation and collaboration of state agencies in the planned events, ensuring inclusivity of resources and partners.
- *Supplemental Activities in Schools/Districts*: Evaluate the engagement of individual schools and districts in augmenting core events with supplemental activities, providing resources for creative and educational initiatives.
- *Engagement of SICs/PTOs*: Assess the engagement of local SICs/PTOs as stakeholders and their involvement in core events, raising awareness among parents about the value of cyber education.
- *Partnerships with Private Sector and Non-profits*: Track the establishment of partnerships with private sector companies and non-profits, assessing their support in terms of resources and financial assistance for early cyber awareness programs.
- *Cross-District Collaboration Promotion*: Measure the promotion of cross-district collaboration within the established framework, encouraging the sharing of best practices, challenges, and successful engagement models.

Metrics of Effectiveness:

- *Increased Cyber Awareness*: Evaluate the effectiveness of the initiative in increasing cyber awareness among students, parents, and communities.
- *Family Participation in Events*: Measure the level of family participation in core events, specifically assessing engagement with events designed to appeal to the entire family.
- *Private Sector and Non-profit Impact*: Assess the impact of private sector and non-profit partnerships on enhancing the initiatives, considering the support provided in terms of resources and financial assistance.
- *Knowledge Retention and Application*: Evaluate the retention and application of cyber knowledge among students as a result of the early awareness programs.
- *Framework Adoption Across Districts*: Track the adoption of the established framework for cross-district collaboration and assess its impact on creating a supportive and collective learning environment.

5. Facilitate Adoption of Cyber Education Assets at SC Technical Colleges

- ***Align:*** *Leverage successes and lessons learned among South Carolina's technical colleges to facilitate the growth of cyber education assets and infrastructure across the SC Technical College System*
- ***Augment:*** *Elevate the baseline of cybersecurity education assets and capabilities across the South Carolina Technical College System to enhance the state's cyber education landscape*
- ***Attract:*** *Position South Carolina as a premier source of accessible and transformative post-secondary cybersecurity education to attract workforce aspirants, investments, and private sector partnerships*

The escalating demand for cybersecurity expertise necessitates a proactive approach in equipping our workforce with relevant skills. This need extends beyond K-12 education, highlighting the importance of South Carolina's technical colleges in bridging the gap between foundational knowledge and advanced, practical cybersecurity skills. By integrating state-of-the-art cyber education capabilities with an expanded array of foundational assets, these institutions can offer students immersive learning experiences that mirror real-world cyber environments. And while some of the state's technical colleges have distinguished themselves by gaining federally recognized certifications for academic excellence and/or developing advanced educational assets, we envision a landscape in which every South Carolinian resides within a feasible commuting distance of a "cyber-forward" technical college.

As part of this strategic planning process, a survey was administered (in partnership with the SC Commission on Higher Education) to South Carolina's colleges and universities, with nearly 60% of them responding. From this survey, several key insights emerged regarding gaps in cyber education assets:

- *Hiring Instructors*: The most pressing challenge in securing quality cybersecurity teachers is offering competitive compensation, followed by the difficulty in sourcing the requisite cyber expertise and teaching experience.
- *Scholarships*: Only 28% of responding institutions currently offer cyber-specific scholarships for students.
- *Dual-Credit Courses*: Fewer than half of the responding institutions offer dual-credit cybersecurity courses, allowing high school students to earn college credits and gain early exposure to cybersecurity.
- *Student Work Experience*: Responding institutions estimate that only 39% of cybersecurity graduates have relevant work experience before graduating.
- *Infrastructure for Practical Training*: Only 30% of responding schools have a cyber range via which students can experience practical, hands-on learning, while only 27% possess a Security Operations Center (SOC) or Network Operations Center (NOC) where students can gain cyber work experience.

These insights underscore the importance of addressing both education and infrastructure asset gaps to enhance the cybersecurity talent pipeline in South Carolina. Fortunately, some of our institutions have taken the steps to develop advanced assets, programs, and capabilities. We must provide additional resourcing and coordination to help these trailblazers develop "playbooks" based upon their successes and lessons learned, in order to promulgate the adoption of these assets across the technical college system. Along the way, collaboration with cybersecurity companies and industry experts can be transformative. These partnerships can facilitate the acquisition of advanced cyber tools, the development of simulation environments, and the expansion of internship and apprenticeship opportunities for hands-on learning and work experience.

The resulting landscape will not only more effectively prepare students for immediate employment but also foster a culture of continuous learning and professional growth while positioning our state as a premier destination for accessible cyber education and career transition.

Key Partners: South Carolina Technical College System (SCTCS; incl. Apprenticeship Carolina), SC Department of Employment and Workforce, SC Technical College faculty and administration, SC cybersecurity companies, SC industry experts

Key Tasks:

- Partner with cybersecurity companies and industry professionals to identify and procure advanced cyber education assets for technical colleges.
- Collaborate with partners to develop and refine cybersecurity curricula that incorporate practical, hands-on training with state-of-the-art tools and simulations.
- Encourage and support schools in aligning their cybersecurity programs with the NICE Workforce framework to ensure industry relevance and applicability.
- Provide training and professional development opportunities for technical college educators to effectively utilize new cyber education assets.
- Establish dedicated cyber labs and simulation environments within technical colleges to facilitate immersive, experiential learning.
- Launch outreach campaigns to attract students, highlighting the enhanced cybersecurity education and training opportunities available at SC technical colleges.
- Continuously assess the effectiveness of adopted cyber education assets and make necessary adjustments to ensure alignment with industry needs and tech advancements.
- Expand dual-credit offerings to high school students, allowing students to earn college credits and gain early exposure to cybersecurity principles and practices.
- Establish and promote scholarships specifically for cybersecurity students to attract and support those pursuing careers in the field while reducing financial barriers.
- Coordinate via SC Department of Employment and Workforce and Apprenticeship Carolina to onboard additional cybersecurity companies in apprenticeship and internship programs and strengthen those companies' relationships with technical colleges.
- Develop a system to monitor student progress and outcomes from apprenticeships and internships. Including skill development, job placements, and career advancement.

Metrics of Performance:

- *Adoption Rate of Cyber Assets*: Track the number of technical colleges integrating new cyber education assets into their programs.
- *Industry Partnerships Formed*: Measure the number and quality of partnerships established with cybersecurity companies and industry experts.

- *Educator Training Hours*: Quantify the hours of professional development provided to educators on the use of new cyber education assets.
- *Infrastructure Development*: Assess the establishment and utilization of dedicated cyber labs and simulation environments.
- *Scholarship Distribution*: Measure the number and value of cyber-specific scholarships awarded to students.
- *NICE Framework Alignment*: Evaluate the extent to which technical colleges map their cybersecurity programs to the NICE Workforce framework.
- *Number of Apprenticeship and Internship Programs Established:* Track the number of new apprenticeship and internship programs developed in partnership with cybersecurity companies and organizations.
- *Student Participation Rates:* Measure the number of students participating in apprenticeship and internship programs annually.
- *Program Completion Rates:* Monitor the percentage of students who successfully complete their apprenticeships and internships.

Metrics of Effectiveness:

- *Student Enrollment*: Monitor the increase in student enrollment in cybersecurity programs at technical colleges.
- *Student Competency*: Evaluate improvements in student competency in cybersecurity skills through assessments and industry certifications.
- *Dual-Credit Participation*: Track the number of high school students participating in dual-credit cybersecurity programs.
- *Job Placement Rates*: Measure the job placement rates of graduates in cybersecurity roles within the industry.
- *Employer Feedback*: Gather feedback from employers regarding the preparedness and skill levels of graduates from SC technical colleges.
- *Curricula Relevance*: Ensure cybersecurity curricula remains current and relevant by periodically reviewing and updating course content.
- *Sustainability of Programs*: Assess the sustainability and scalability of the cyber education programs and assets, ensuring long-term benefits for students and the broader community.
- *Skill Acquisition*: Assess improvements in students' cybersecurity skills and competencies through pre- and post-apprenticeship/internship program evaluations.
- *Retention Rates*: Monitor the retention rates of former apprentices and interns within the cybersecurity industry.
- *Student Feedback*: Gather feedback from students regarding their experiences in apprenticeship and internship programs to identify strengths and areas for improvement.
- *Impact on Cybersecurity Workforce*: Assess the overall contribution of apprenticeship and internship programs to addressing the cybersecurity workforce gap in South Carolina.

6. INSTITUTE A STATEWIDE CYBERSECURITY CAPSTONE PROJECT FRAMEWORK

- ***Align:*** *Promote a unified approach to industry participation in cybersecurity education across South Carolina while increasing alignment between academic outcomes and private sector needs.*
- ***Augment:*** *Build upon the success of existing cyber capstone programs to promulgate their use across South Carolina.*
- ***Attract:*** *Strengthen South Carolina's cyber workforce readiness to increasingly appeal to cybersecurity students and executives.*

Some institutions of higher education (IHEs) in South Carolina require cybersecurity students to successfully complete a capstone project as part of their graduation degree or certificate requirements. While the specific nature and duration of these projects vary, they can incorporate private sector collaboration, with students putting their training and education to the test by undertaking cyber-related tasks in support of a cybersecurity company. In addition to enabling students to explore the practical application of their academic gains, such projects are instrumental in enhancing connectivity between academia and industry—strengthening the state's cyber workforce pipeline while further aligning educational outcomes with employer needs.

We must promote wholesale adoption of this practice across all South Carolina IHEs and equip our schools with a repeatable framework to efficiently establish and effectively manage their capstone programs. We have already initiated a survey of technical colleges and universities across the state to identify those with existing capstone programs so that we may engage them to identify best practices, areas for improvement, and means of developing a playbook for other schools to follow. We must also engage their private sector partners to identify key enablers and impediments to participation so that we may improve the value to industry, expand the roster of participating cybersecurity companies, and increasingly connect today's students with tomorrow's employers.

Key Partners: SC Department of Employment and Workforce, South Carolina Commission on Higher Education, SC Technical College System, SC universities, SC cybersecurity companies

Key Tasks:

- Engage IHEs with existing capstone programs and their industry partners to identify best practices and areas for improvement.
- Develop cyber capstone program "playbook" for SC IHEs to implement new cyber capstone programs and/or improve existing programs.
- Emplace centralized resources to assist IHEs with establishing, managing, and securing industry partners for their cyber capstone programs and for promoting private sector awareness and participation.

Metrics of Performance:

- *Engagement with Existing Capstone Programs*: Measure the level of engagement with IHEs having existing capstone programs and their industry partners to identify best practices and areas for improvement.

- *Development of Capstone Program "Playbook"*: Assess the completion and quality of the cyber capstone program "playbook" developed for South Carolina IHEs.
- *Establishment of Centralized Resources*: Track the establishment of centralized resources to assist IHEs in establishing, managing, and securing industry partners for their cyber capstone programs.

Metrics of Effectiveness:

- *Implementation of New Capstone Programs*: Measure the number of South Carolina IHEs that have implemented new cyber capstone programs based on the developed playbook.
- *Improvement of Existing Capstone Programs*: Assess the extent to which existing cyber capstone programs in South Carolina IHEs have improved based on the identified best practices.
- *Industry Partner Engagement*: Evaluate the success of centralized resources in assisting IHEs with securing industry partners and promoting private sector awareness and participation.
- *Private Sector Participation Rates*: Track the participation rates of private sector entities in South Carolina IHE cyber capstone programs.
- *Feedback from IHEs*: Gather feedback from IHEs on the effectiveness and usefulness of the developed playbook and centralized resources.

III. Posture & Readiness

- **Making cybersecurity guidance, resources, and support accessible to South Carolina residents, agencies, companies, and organizations**

Between phishing scams that threaten the financial security of individuals, massive data breaches that expose personally identifiable information, ransomware attacks that cripple organizations, and hacks that enable unauthorized control of critical physical systems, the potential impacts of cybercrime are manifold and severe. Add to that the threats posed by international actors seeking to sow misinformation, steal intellectual property, or achieve political goals through online disinformation, and our increasing digital connectivity and dependence upon information systems represents a rapidly expanding threat vector for which we must ensure we are sufficiently postured.

Broadly speaking, we must be prepared to combat these threats on two fronts: by raising the collective cyber awareness and proficiency of our residents and organizations, and by ensuring the timely provision of technical resources and services to assist those impacted by cyber incidents. By strengthening our state's cybersecurity posture and readiness across the full risk management framework of "identify, protect, detect, respond, and recover," we can improve the security of information systems, networks, devices, and applications used by South Carolina residents and organizations.

7. Fund and Expand the SC Critical Infrastructure Cybersecurity Program

- ***Align:*** *Ensure the presence of a centralized resource to coordinate cybersecurity guidance and assistance to stakeholders across South Carolina.*
- ***Augment:*** *Enable SC CIC to expand its positive impact on South Carolina's cyber landscape by growing its technical capabilities and workforce.*
- ***Attract:*** *Demonstrate South Carolina's commitment to providing resources and assistance to help residents and organizations secure their digital networks and infrastructure.*

The South Carolina Critical Infrastructure Cybersecurity (SC CIC) Program, housed within the South Carolina Law Enforcement Division (SLED), is one of the state's strongest cyber assets. Focused on providing cybersecurity guidance, resources, and support to critical infrastructure (CI) operators across South Carolina, SC CIC offers robust capabilities for cyber threat information sharing, risk assessment, awareness training, tabletop exercises, and incident response—all at no cost to those organizations. Since 2021, SC CIC has expanded its Cyber Liaison Officer (CLO) network—comprised of designated cyber representatives from the state's CI entities—by 250%, now standing at over 430 CLOs. These members participate in monthly information exchanges and trainings, benefit from threat alerts and advisory communications, and improve their organization's security posture by completing readiness exercises—all facilitated by SC CIC. In 2023 alone, the organization responded to 27 CI cyber incidents (including 20 within the Government sector) and scanned over 750 malware samples to inform upon cyber threat intentions and capabilities. Also in 2023, SC CIC led the state's efforts to secure over $3.5M in federal funding to improve the cybersecurity of South Carolina's local government entities.

Despite its critical role, however, SC CIC remains overly dependent on securing federal grant funds to supplement its SLED-allocated budget, simply to sustain its current operational footprint with minimal staffing. As South Carolina embarks upon its current path to prioritizing improved cybersecurity across the ecosystem, it must provide additional resources to sustain and strengthen what is arguably the state's "crown jewel" for cyber preparedness and incident prevention. The success of this strategic plan requires a centralized resource that is adequately positioned and able to coordinate technical assistance to a wide range of public and private stakeholders. SC CIC has already demonstrated that it has the capability—but we must ensure it also has the requisite capacity to do so in an even more expanded role. Dedicated state funding is needed to ensure the organization can grow its technical capabilities to keep pace with the cyber threat landscape; grow its staff to include regional cyber advisors who can nurture critical relationships and coordinate technical support across the state; and respond in a timely manner to an expanded customer base.

Key Partners: South Carolina Law Enforcement Division, SC Office of the Governor, SC legislature

Key Tasks:

- Review and approve dedicated SC CIC budget request (already submitted).
- Codify expanded roles and responsibilities for SC CIC within the scope of this strategic plan.

Metrics of Performance:

- *Budget Approval Timeline*: Measure the timeline for reviewing and approving the dedicated SC CIC budget request.
- *Implementation of Expanded Roles*: Track the implementation timeline for codifying expanded roles and responsibilities for SC CIC within the scope of the strategic plan.

Metrics of Effectiveness:

- *Increased State Funding*: Assess the success of securing dedicated state funding for SC CIC to sustain and strengthen its operational capabilities.
- *Growth in Technical Capabilities*: Measure the growth in technical capabilities of SC CIC to keep pace with the evolving cyber threat landscape.
- *Staff Expansion*: Evaluate the success of SC CIC in growing its staff, specifically regional cyber advisors, to nurture critical relationships and coordinate technical support across the state.
- *Timely Response to Customer Base*: Assess the ability of SC CIC to respond in a timely manner to its expanding customer base, considering the increased demand for cybersecurity assistance.
- *Enhanced Coordination with Stakeholders*: Measure the effectiveness of SC CIC in coordinating resource provisioning and technical assistance to a wide range of public and private stakeholders.
- *Customer Satisfaction*: Gather feedback from stakeholders, including critical infrastructure operators, on their satisfaction with the services provided by SC CIC.

8. PROMOTE CYBERSECURITY READINESS ACROSS SC'S INDUSTRY SUPPLY CHAIN

- ***Align:*** *Ensure equitable access to critical cybersecurity guidance and resources for all South Carolina companies.*
- ***Augment:*** *Complement South Carolina's state agency and large business cyber readiness by improving the posture of smaller enterprises.*
- ***Attract:*** *Strengthen South Carolina's commercial competitiveness by decreasing the cyber risk surface of our supply chain.*

The ever-increasing digital interconnectivity of our world brings with it an ever-expanding risk surface for cyber threats. Organizations cannot simply look inwards to secure their own networks, systems, devices, and data—they also face vulnerabilities from every digital touchpoint with an external entity, resulting in a cascading host of threat vectors to be managed and monitored. Indeed, large organizations within South Carolina have experienced cyber incidents that originated downstream in their supply chains, as threat actors exploited vulnerabilities in small suppliers' postures. Accordingly, organizations sitting atop those supply chains typically require their vendors to certify compliance with established cybersecurity requirements. This approach, however, ensures only that the vendors attest to cybersecurity compliance, rather than achieve it—which serves only to establish liability in case of a future cyber breach, not actually decrease the likelihood of that breach.

Technology executives at some of South Carolina's largest employers have shared their insights on the cybersecurity postures within their supply chains in a way that paints a picture of three discrete vendor categories. First are large and some medium-sized businesses that have the financial and personnel resources to achieve cybersecurity compliance as needed. Second are most medium-sized and some small businesses that generally know what must be done but may lack the resources to fully emplace every desired solution or process—requiring them to assess risk trade-offs and prioritize partial solutions. Third are many small businesses that also lack the resources to emplace all desired solutions—but more concerningly, they do not readily understand what must be done or how to go about addressing the requirements in the first place. In many cases, these smaller businesses seek guidance and support from their large partners atop the supply chain, who do not have the time or resources to advise dozens (if not hundreds) of vendors on their individual cybersecurity investments.

When asked what the state of South Carolina can do to help address cyber risk in the lower half of their supply chains, those same executives provided a consistent answer: Provide centralized, easy-to-follow guidance and resources—and support, where possible—for small businesses. Unfortunately, many existing resource websites take an encyclopedic approach to providing cybersecurity guidance, highlighting links to dozens of conceptual frameworks, recommended policies, and secondary information sources. Non-tech-savvy small business owners are seeking direct guidance, not an overwhelming list of references in a technical field with which they are unfamiliar. South Carolina must arm its small business owners with actionable guidance that can help them navigate the complexity of cybersecurity preparedness, leveraging the expertise of SC CIC (see previous item) and housed within a centralized state portal for cyber information (see next item). Concerns of perceived liability—i.e., if a vendor is hacked despite following the South Carolina website guidance—

must be appropriately addressed but need not prevent us from providing critical assistance to our resident industries.

Key Partners: SC Department of Commerce, SC CIC, SC Department of Administration, SC Manufacturing Extension Partnership

Key Tasks:

- Develop and implement a centralized state portal for cyber information aimed at small businesses, providing easy access to actionable guidance on cybersecurity preparedness.
- Collaborate with SC CIC to leverage its expertise in developing targeted cybersecurity resources specifically tailored for small businesses within the industry supply chain.
- Establish a support system to assist small businesses in understanding and implementing cybersecurity best practices, addressing their specific challenges and needs.
- Conduct outreach and awareness campaigns targeting small businesses within the industry supply chain, emphasizing the importance of cybersecurity and the available state resources.
- Facilitate collaboration between large organizations and their smaller suppliers, creating a framework for sharing best practices and providing mutual support in enhancing cybersecurity postures.
- Consider highlighting in-state cybersecurity vendors (e.g., on the cyber resource portal and in awareness and outreach events) to promote the growth of South Carolina's cyber industry landscape.
- Monitor and evaluate the effectiveness of the guidance and support provided, collecting feedback from small businesses, and adjusting strategies accordingly to ensure continuous improvement.

Metrics of Performance:

- *Implementation of Centralized State Portal*: Measure the successful development and implementation of the centralized state portal for cyber information aimed at small businesses.
- *Collaboration with SC CIC*: Assess the level of collaboration with SC CIC in leveraging their expertise to develop targeted cybersecurity resources for small businesses in the industry supply chain.
- *Establishment of Support System*: Track the establishment of a support system to assist small businesses in understanding and implementing cybersecurity best practices, addressing their specific challenges and needs.
- *Outreach and Awareness Campaigns*: Evaluate the reach and impact of outreach and awareness campaigns targeting small businesses within the industry supply chain.
- *Facilitation of Collaboration between Organizations*: Measure the success in facilitating collaboration between large organizations and their smaller suppliers, creating a framework for sharing best practices and mutual support in enhancing cybersecurity postures.

- *Monitoring and Evaluation System*: Assess the effectiveness of the monitoring and evaluation system in place to collect feedback from small businesses and adjust strategies accordingly.

Metrics of Effectiveness:

- *Increased Small Business Cyber Preparedness*: Evaluate the impact of the initiative on increasing cyber preparedness among small businesses in the industry supply chain.
- *Number of Small Businesses Engaged*: Measure the number of small businesses engaged through the centralized state portal, support system, and outreach campaigns.
- *Collaboration Success Metrics*: Assess the success of collaboration between large organizations and their smaller suppliers by tracking the adoption of shared best practices and mutual support measures.
- *Feedback and Satisfaction*: Gather feedback from small businesses on the guidance and support provided, assessing their satisfaction and areas for improvement.
- *Reduction in Cybersecurity Incidents*: Evaluate the impact on reducing cybersecurity incidents among small businesses in the industry supply chain.
- *Continuous Improvement*: Measure the success in achieving continuous improvement by adjusting strategies based on feedback and evaluation results.

9. LAUNCH A CENTRALIZED WEBSITE FOR SOUTH CAROLINA CYBERSECURITY RESOURCES

- ***Align:*** *Promote equitable access to cyber ecosystem resources for all South Carolina residents and organizations while improving the reach and effectiveness of those resources.*
- ***Augment:*** *Improve South Carolinians' ability to access and leverage cybersecurity resources, guidance, and support in order to strengthen our collective cyber posture.*
- ***Attract:*** *Demonstrate South Carolina's commitment to elevating cybersecurity across our state and creating an increasingly secure environment for industry, investment, and quality of life.*

In any strategic initiative, the impact of even the most well-intentioned and right-sized resources can be severely limited if those resources are not effectively positioned for public engagement. And in the case of a highly technical field—like cybersecurity—that can feel overly complex to newcomers, the entire user experience surrounding those resources must be designed for maximum ease, efficiency, and clarity. Because many of the cyber growth initiatives to date in our state are tied to local and/or highly dispersed champions and efforts, it is difficult for South Carolinians to become informed on the breadth of those activities and the opportunities they present. Students and parents seeking information on cyber education may not know what CAE certification is or how to identify the South Carolina technical colleges and universities possessing that designation. Small business owners may know they need to comply with industry standards but do not know how to get started. Organizational managers may suspect they may have experienced a cyber breach, but are not sure what it means, what do to, or who to notify.

While a subset of those informational resources can be found on various websites hosted by federal agencies, those sites tend to favor an encyclopedic approach (e.g., providing links to 20 other sites listing various combinations of cyber best practices) over an actionable one (e.g., providing a concise list of steps to be taken). In addition, reliance upon nationally oriented sites does not help South Carolinians understand the resources and opportunities available to them in their own backyard. For our strategic plan to realize the intended impact, and to maximize the reach and effectiveness of each item within it, we must provide a "one-stop-shop" web portal where students, parents, guidance counselors, workers, entrepreneurs, executives, and investors can easily find the information they need and connect with relevant in-state resources. The site should enable users to report cyber incidents; find cyber policy and implementation guidance; understand cyber learning pathways and identify educational opportunities; explore cyber internship, apprenticeship, and job openings; connect with cyber innovation activities; leverage career transition programs for military veterans; and more. Importantly, the information housed within this site must be shaped and provided in a way that is easily accessible and user-friendly to those audiences—meaning it must favor simplicity and storytelling over complexity and data provision.

The South Carolina Office of Regulatory Staff, Broadband Office, should be a critical partner in this activity, as its 2024 Digital Equity Plan includes "online privacy and cybersecurity" as one of its five overarching goals. The plan specifies an objective of every resident of South Carolina being able to utilize broadband services safely and securely.

Key Partners: SC Department of Commerce, SC Office of Regulatory Staff (Broadband Office), SC Council on Competitiveness, SC Department of Employment and Workforce, SC Department of Education, SC Commission on Higher Education, SC CIC, SC Department of Administration, SC Manufacturing Extension Partnership, SC Research Authority, SC Department of Veterans Affairs, SC Department of Consumer Affairs

Key Tasks:

- Determine which strategic planning items warrant inclusion within the website and how (e.g., which information, static versus dynamic content, interactivity).
- Ensure coordination with cyber ecosystem branding & marketing item within the Industry Growth pillar to shape design, content, and functionality.
- Determine scope and functional requirements of website and "owning" agency.
- Identify web developer (in-house or vendor).
- Work with developer to design site and engage partners to build content.
- Identify necessary and suitable content developers and emplace a content update (review and refresh) schedule to ensure information remains appropriately up to date.

Metrics of Performance:

- *Inclusion of Strategic Planning Items*: Track the successful determination and inclusion of relevant strategic planning items within the website.
- *Coordination with Cyber Ecosystem Branding & Marketing*: Assess the level of coordination with the cyber ecosystem branding and marketing item within the Industry Growth pillar to shape the design, content, and functionality of the website.
- *Scope and Functional Requirements Definition*: Measure the successful determination of the scope and functional requirements of the website, including clarity on the owning agency.
- *Identification of Web Developer*: Track the timely identification of a web developer, either in-house or through a vendor.

- *Website Design and Development*: Assess the progress made in designing the website and engaging partners to build content.

Metrics of Effectiveness:

- *User Engagement*: Evaluate the level of user engagement with the centralized website for South Carolina cyber resources, including the number of visitors, time spent on the site, and page views.
- *Relevance of Content*: Assess the relevance and usefulness of the content on the website, based on user feedback and analytics.
- *Interactivity and User Experience*: Measure the effectiveness of interactivity features and overall user experience, ensuring that the website meets the needs of its target audience.
- *Branding Alignment*: Evaluate how well the website aligns with the branding and marketing efforts of the broader cyber ecosystem, ensuring consistency and synergy.
- *Accessibility and Inclusivity*: Assess the accessibility and inclusivity of the website, ensuring that it is user-friendly for individuals with diverse needs and backgrounds.
- *Partner Engagement*: Measure the success of engaging partners in contributing content to the website and the variety of resources provided.
- *Timely Launch*: Track the timely launch of the centralized website.

IV. Industry Growth

- **Making a supportive enabling asset environment accessible to cybersecurity companies and entrepreneurs in South Carolina**
- **Making leading cybersecurity products and services accessible to individuals and organizations throughout South Carolina**

Cybersecurity as an industry is not in competition with South Carolina's legacy and leading industries, but rather is a key enabler for sustaining the operational resilience and economic competitiveness of incumbent firms. As manufacturing, supply chain management, life sciences, and even agriculture increasingly embrace digital connectivity, our state's economy is increasingly vulnerable to cybersecurity risks. We must provide an attractive and supportive environment for cybersecurity companies to originate, relocate, and grow in South Carolina to furnish our resident organizations with the expertise, products, and services they need to manage those risks. In addition to supporting the resilience of our industrial base, cybersecurity companies also represent an outsized contributor to our economy, as cyber professionals in South Carolina command earnings up to 240% higher than the state's median wage.

This imperative to grow the cybersecurity industry footprint within our state supports—and is supported by—the other lines of effort within this strategic plan. To effectively strengthen our collective cyber posture and readiness, grow an enviable and sustainable cyber workforce, unlock transformational cyber technical innovation, and provide leading capabilities and expertise to support state and national defense missions, South Carolina must be home to a robust cybersecurity industry that in turn is strengthened by the other enabling aspects of the state's cyber ecosystem.

10. Develop and Market South Carolina's Cyber Ecosystem Brand to Promote Economic Development

- ***Align:*** *Ensure efforts to strengthen our cyber ecosystem properly support an overarching vision for South Carolina's sustained security and prosperity while also enhancing our economic development.*
- ***Augment:*** *Maximize the impact of South Carolina's cyber growth initiatives through effective communication to engender increased awareness and participation across our state.*
- ***Attract:*** *Effectively communicate South Carolina's cyber growth vision to external stakeholders to attract critical resources for workforce, business, and capital growth.*

Even the most well-designed and well-executed efforts can fail to meet their objectives if they are not supported by effective communications. In the case of strategic initiatives such as this one, it is not enough to list the individual actions being taken and parcel out their communications to each lead agent. Rather, each activity must be presented as a supportive part of a larger whole, and this larger whole must be explained similarly across all the supporting narratives. The resulting consistency helps stakeholders to visualize the desired end state, place increased trust in the collective processes and road maps to get there, and understand how their contributions to any one activity will help enable the larger outcome. At the same time, this overarching narrative is important to help people and organizations understand why they should support this initiative, potentially at the expense of another competing effort. In this case, why should they contribute their time, talents, or money to help grow South Carolina's cyber ecosystem, and what differentiates our desired end state from other state or regional cyber capacity-building efforts? To answer these questions and engender buy-in, we need to develop and communicate our cyber ecosystem "brand."

As more states across the country have crafted similar narratives in recent years, they have tended to feature one or more pillars—such as education, military and defense, or corporate attraction—as the central point of their cyber ecosystem's brand. Just as often, states tout a "whole-of-state" cyber strategy that is limited to addressing state and local government needs, without a fuller consideration of the needs of residents, private organizations, or the enabling assets that are required for sustained growth and performance. Based on the inventory and assessment we have conducted of South Carolina's cyber ecosystem and the many conversations that have informed this strategic plan, it is this comprehensiveness that sets us apart. We are investing in the totality of the enabling assets required to grow a thriving and sustainable cyber workforce, industry, and innovation landscape, while providing cyber guidance and support to the full range of people and organizations within our state. We are emplacing and augmenting the assets necessary to grow tomorrow's cyber workers, to equip tomorrow's cyber innovators, and to support tomorrow's cyber companies—all while ensuring that this critical horizontal capability can be fully leveraged by South Carolina's industries, households, and government offices for increased security, resilience, and economic growth.

We must develop this brand to resonate with top-tier cybersecurity and defense talent, specifically including leading companies in these industries. By showcasing our strategic geographic location, state-of-the-art research facilities, and business-friendly environment, we can create a compelling proposition for cyber and defense entities to relocate to and expand their operations within our state. Our cyber brand must also align with and support our state's push in the advanced energy sector as marketed via the SC Nexus initiative. As energy generation, distribution, and storage systems become more technologically advanced and interconnected, they also become more vulnerable to cyber-attacks. Cybersecurity initiatives can develop robust protocols and defenses to shield critical infrastructure, especially in the enhancement of grid integration and management systems.

To engender the necessary buy-in and enable the collective success of this initiative, we must fully flesh out this narrative and ensure it properly supports—and is supported by—the narratives surrounding each component activity. We must equip our growth agents with the materials and insights necessary to effectively communicate this brand and its value proposition to audiences both inside and outside of South Carolina. In addition to enabling external clarity on our vision and value, this cohesive brand will serve as a touchstone for ensuring that our day-to-day efforts are appropriately aligned with each other and the bigger picture.

Key Partners: SC Department of Commerce, SC Council on Competitiveness, SC Department of Employment and Workforce, SC Department of Education, SC Research Authority, SC Department of Veterans Affairs, SC Department of Consumer Affairs

Key Tasks:

- Define the overarching narrative and brand identity for South Carolina's cyber ecosystem, emphasizing its comprehensiveness and differentiation from other state initiatives.

- Articulate the value proposition of South Carolina's cyber ecosystem brand, highlighting its focus on growing a thriving and sustainable cyber workforce, industry, and innovation landscape.
- Engage key stakeholders, including government agencies, industry partners, educational institutions, and community organizations, to gather input and build consensus around the brand narrative.
- Develop a messaging strategy that communicates the brand narrative consistently across all communications channels and materials.
- Create content, such as website copy, brochures, presentations, and social media posts, that effectively communicates the value and objectives of South Carolina's cyber ecosystem brand.
- Establish brand guidelines to ensure consistency in visual identity, tone of voice, and messaging across all brand-related materials and communications.
- Provide training and resources to stakeholders and growth agents to effectively communicate the brand narrative and value proposition to internal and external audiences.
- Develop marketing campaigns to raise awareness of South Carolina's cyber ecosystem brand and attract attention from target audiences, including potential investors, businesses, and talent.

Metrics of Performance:

- *Definition of Narrative and Brand Identity*: Measure the successful definition of the overarching narrative and brand identity for South Carolina's cyber ecosystem.
- *Articulation of Value Proposition*: Assess the clarity and effectiveness of articulating the value proposition of South Carolina's cyber ecosystem brand, emphasizing its focus on workforce, industry, and innovation.
- *Engagement with Key Stakeholders*: Track the level of engagement with key stakeholders to gather input and build consensus around the brand narrative.
- *Development of Messaging Strategy*: Measure the development of a messaging strategy that communicates the brand narrative consistently across all communications channels and materials.
- *Creation of Brand Content*: Evaluate the creation of content, such as website copy, brochures, presentations, and social media posts, to effectively communicate the value and objectives of the cyber ecosystem brand.
- *Establishment of Brand Guidelines*: Track the establishment of brand guidelines to ensure consistency in visual identity, tone of voice, and messaging across all brand-related materials and communications.
- *Training and Resources Provided*: Measure the provision of training and resources to stakeholders and growth agents to effectively communicate the brand narrative and value proposition.
- *Hosting Premier Cybersecurity Events*: Track the regularity and growth of South Carolina’s cyber industry events (e.g., SC Decoded, South Coast Cyber Summit), at which we position our state as a focal point for national and international cybersecurity dialogue and networking.

Metrics of Effectiveness:

- *Brand Awareness*: Assess the level of awareness of South Carolina's cyber ecosystem brand among target audiences, including potential investors, businesses, and talent.
- *Perception Survey*: Conduct surveys or focus groups to gauge stakeholders' perception of the brand narrative and its alignment with the state's cyber ecosystem objectives.
- *Consistency in Communication*: Evaluate the extent to which stakeholders and growth agents adhere to the established brand guidelines in their communication efforts.
- *Stakeholder Engagement*: Measure the level of stakeholder engagement and collaboration in promoting and reinforcing the cyber ecosystem brand.
- *Impact on Attraction and Retention*: Assess the impact of marketing campaigns on attracting businesses, investors, and talent to South Carolina's cyber ecosystem, as well as retaining existing stakeholders.
- *Partnership Formation*: Track the formation of partnerships and collaborations with external organizations and entities as a result of brand promotion efforts.
- *Global Ranking Improvements:* Monitor South Carolina's rankings in national and international lists of top cybersecurity and defense hubs.

11. EXPAND EZONE APPLICABILITY TO INCENTIVIZE CYBERSECURITY UPSKILLING

- ***Align***: *Ensure existing resources for corporate growth in South Carolina are positioned to support cyber capacity-building across our industries.*
- ***Augment:*** *Improve the ability of South Carolina companies to secure their networks, systems, devices, and data through increased cybersecurity training at decreased cost.*
- ***Attract:*** *Provide incentives for companies to originate in, relocate to, and/or expand in South Carolina while benefitting from a supportive cybersecurity ecosystem.*

The Enterprise Zone Retraining Program (EZone), through the SC Technical College System, offers a tax incentive (against employee withholdings) to South Carolina companies that incur approved training costs to upskill employees in association with new equipment and/or technologies. The program has been designed to support the development of "first-line" workers in manufacturing, processing, and technology-intensive companies, but could be expanded to help improve the cybersecurity and resilience of the state's industry at large. There are two ways in which EZone can be relevant to training cybersecurity professionals: one that is currently applicable (but perhaps not well known to cybersecurity companies), and one that is not (but which we seek to initiate).

To qualify for EZone-related tax incentives, companies must incur costs to train full-time employees (or immediate supervisors thereof) who have been on the company payroll for at least two years, are offered benefits/healthcare through the company, and require training or new equipment and/or processes. Cybersecurity professionals who work at cybersecurity companies and meet the above criteria (e.g., they are "first-line" employees—meaning they actively deliver cybersecurity services to customers) currently qualify as approved recipients of EZone-approved training. For example, an Information Security Analyst working at a South Carolina cybersecurity provider who monitors corporate customers' networks may require upskilling to attain a higher technical certification or implement a new piece of software—and that training would qualify for EZone, provided the above conditions are all met. However, because the program was originally designed to benefit (and seems to be marketed towards) manufacturing and processing companies, cybersecurity companies may not realize that EZone tax credits are potentially available to them. In fact, three of the industry (NAICS) codes eligible for EZone tax incentives—541511, 541512, and 518210—include cybersecurity products or services, meaning that SC companies operating under those codes may already be eligible to train their cyber workers through the EZone program.

While the scenario described above applies only to cybersecurity workers at cybersecurity companies who are delivering services to external customers; it does not apply to other types of companies seeking to improve their internal cybersecurity capabilities and posture—a key aim of our statewide cyber strategy. To address this, we propose to expand EZone applicability to include cybersecurity professionals at any kind of SC company who support that company's internal cybersecurity needs. In keeping with EZone's current intent, this would be limited to "first-line" employees and their supervisors—we are not proposing to offer tax credits to companies to train their Director of Information Technology, for example. In addition to helping existing companies in our state strengthen their cybersecurity, this EZone expansion would demonstrate that South Carolina is a supportive home for companies seeking to relocate and expand within an ecosystem that values the resilience of its industry partners.

Key Partners: SC Technical College System, SC legislature, SC Department of Commerce, SC Department of Employment and Workforce, SC Council on Competitiveness, SC Small Business Development Centers

Key Tasks:

- Update EZone marketing language on SCTCS website and supporting materials to clarify current applicability to cybersecurity firms.
- Actively communicate program applicability to SC cybersecurity firms.
- Draft formal language to propose EZone expansion through SC legislature.
- Socialize concept and return on investment, identify legislative sponsor(s).

Metrics of Performance:

- *Update of EZone Marketing Language*: Measure the successful update of EZone marketing language on the SCTCS website and supporting materials to clarify current applicability to cybersecurity firms.
- *Communication of Program Applicability*: Track the effectiveness of actively communicating the program's applicability to South Carolina cybersecurity firms through outreach efforts.
- *Drafting of Formal Language for Expansion Proposal*: Measure the completion of drafting formal language to propose the expansion of EZone through the South Carolina legislature.
- *Socialization of Concept and Return on Investment*: Assess the extent to which the concept of EZone expansion and its return on investment are socialized among relevant stakeholders, including potential legislative sponsors.

Metrics of Effectiveness:

- *Awareness Among Cybersecurity Firms*: Evaluate the awareness level among South Carolina cybersecurity firms regarding the expanded applicability of EZone, as indicated by feedback and engagement.
- *Legislative Support*: Measure the level of support garnered from legislators for the proposed expansion of EZone, including the identification of legislative sponsor(s).
- *Legislative Progress*: Track the progress of the proposed expansion through the legislative process, including committee hearings, votes, and eventual passage.
- *Number of Cybersecurity Firms Utilizing EZone*: Measure the increase in the number of cybersecurity firms utilizing EZone incentives for upskilling initiatives as a result of the expansion.
- *Impact on Cybersecurity Workforce Development*: Assess the impact of the expanded EZone program on cybersecurity workforce development in South Carolina, including the number of skilled professionals trained and employed.
- *Economic Impact*: Evaluate the economic impact of the expanded EZone program on the cybersecurity industry in South Carolina, including job creation and business growth.
- *Long-Term Sustainability*: Measure the long-term sustainability of the expanded EZone program, including its ability to continue incentivizing upskilling in the cybersecurity sector.

12. OFFSET INDUSTRY COSTS FOR SECURITY CLEARANCE-RELATED ASSETS

- ***Align***: *Improve South Carolina business access to specialized assets necessary to strengthen their support to DoD cybersecurity missions.*
- ***Augment:*** *Strengthen South Carolina cybersecurity companies' ability to perform classified research and development and secure classified federal contracts.*
- ***Attract:*** *Demonstrate South Carolina's commitment to boosting the competitiveness of resident cybersecurity companies in the federal contracting market.*

The cyber ecosystem study that informed the development of this strategic plan identified that South Carolina lags behind our regional neighbors in terms of the concentration of cybersecurity workers within our state's workforce—and that a main driver of that disparity is the wealth of DoD assets in those states that drive outsized federal contracting opportunities for cybersecurity companies. In order for SC industry to be more competitive at securing those contracts both within our state and beyond its borders, we must boost its access to the specialized resources necessary to compete, win, and deliver on those contracts—to include sensitive compartmented information facilities (SCIFs).

SCIF access is a critical requirement for companies to even be eligible to compete for many federal cybersecurity and cyber-adjacent contracts, much less to actively support those missions and conduct the necessary research and development to grow new corporate capabilities. In turn, that corporate capability growth enhances the overall competitiveness of our state's industry and supports the continuous transformation of our technical innovation landscape. In addition to performing on DoD contracts, SCIF access is necessary to enable our industry to partner with education, workforce development, and innovation stakeholders like the Savannah River National Laboratory, Clemson's National Center for Transportation Cybersecurity and Resilience, and the University of South Carolina Beaufort-led Maritime Cybersecurity Innovation Engine. The strength of our cyber industry in the North Augusta and Aiken areas, in particular, is partially reliant upon our ability to help SC companies effectively compete with firms across the border who can more easily access specialized assets for classified business development and contracting associated with Fort Eisenhower.

Other states that have successfully supported their resident cyber companies—and grown their cyber industry through corporate attraction—have done so by rolling out combinations of the following three SCIF-related tax credits. First, tax credits against costs associated with constructing federally accredited SCIFs in the state. This not only helps medium- and large-sized businesses incur the costs of creating the asset, but also ensures that the asset will reside within South Carolina and support our innovation landscape. Second, tax credits against the costs for small businesses to rent access to SCIFs (perhaps only for the first year) as a requirement of performing on classified federal contracts. While small businesses are not expected to construct their own SCIFs, this tax break would encourage the construction of secure facilities for joint corporate use, enable SC small businesses to more aggressively pursue new contract opportunities, and further enhance our innovation asset landscape. And third, tax credits against the costs of administering personnel security clearance requests to enable SC workers to perform on classified contracts, and for installing and maintaining the specialized information technology needed to process those clearance requests. Some or all of these targeted tax breaks—deployed with annual and/or cumulative ceilings for each qualifying company and for the program overall—can lower the barrier for South Carolina cybersecurity companies to grow their capabilities, revenues, and workforce.

Key Partners: SC Department of Commerce, WesternSC, Charleston Defense Contractors Association, SC Council on Competitiveness, SC Small Business Development Centers

Key Tasks:

- Conduct financial analysis to assess the potential economic impact of the tax credit program on South Carolina's cybersecurity industry, including projected cost savings for businesses and potential revenue growth.
- Advocate for the development and implementation of tax credits to offset costs associated with securing clearance-related assets, such as SCIF construction, rental access, and personnel security clearance requests.
- Develop policies and guidelines for administering the tax credit program, including eligibility criteria, application processes, and annual or cumulative ceilings for qualifying companies.
- Engage with cybersecurity industry stakeholders, including businesses, associations, and educational institutions, to gather input and build consensus on the need for tax credits to support industry competitiveness.
- Implement the tax credit program, including establishing mechanisms for companies to apply for and receive tax credits, and monitoring compliance with program requirements.

- Provide education and outreach efforts to inform eligible companies about the availability of tax credits and how to access them.
- Raise awareness among cybersecurity companies about the importance of securing clearance-related assets for competing in federal contracting opportunities.

Metrics of Performance:

- *Advocacy Efforts*: Measure the level of advocacy efforts made for the development and implementation of tax credits to offset costs associated with securing clearance-related assets.
- *Development of Policies and Guidelines*: Track the completion of policies and guidelines for administering the tax credit program, including eligibility criteria, application processes, and ceilings for qualifying companies.
- *Engagement with Stakeholders*: Assess the extent of engagement with cybersecurity industry stakeholders to gather input and build consensus on the need for tax credits.
- *Financial Analysis Conducted*: Measure the completion of financial analysis to assess the potential economic impact of the tax credit program on South Carolina's cybersecurity industry.
- *Implementation of Tax Credit Program*: Evaluate the implementation of the tax credit program, including the establishment of mechanisms for companies to apply for and receive tax credits, and monitoring compliance.
- *Education and Outreach Efforts*: Track the efforts made to provide education and outreach to inform eligible companies about the availability of tax credits and how to access them.

Metrics of Effectiveness:

- *Number of Tax Credit Applications*: Measure the number of companies that apply for tax credits under the program, indicating interest and participation.
- *Amount of Tax Credits Granted*: Assess the total amount of tax credits granted to qualifying companies, indicating the financial impact of the program.
- *Economic Impact*: Evaluate the economic impact of the tax credit program on South Carolina's cybersecurity industry, including cost savings for businesses and potential revenue growth.
- *Awareness among Cybersecurity Companies*: Measure the level of awareness among cybersecurity companies about the importance of securing clearance-related assets for competing in federal contracting opportunities.
- *Competitiveness in Federal Contracting*: Assess the impact of the tax credit program on the competitiveness of South Carolina's cybersecurity industry in federal contracting opportunities.
- *Feedback from Stakeholders*: Gather feedback from stakeholders on the effectiveness of the tax credit program in offsetting industry costs and supporting competitiveness.

13. SUPPORT TECH TRANSFER BETWEEN NIWC ATLANTIC AND SOUTH CAROLINA INDUSTRY

- ***Align**: Facilitate effective collaboration between South Carolina industry and defense assets and ensure tech transfer initiatives are best positioned to support industry growth.*
- ***Augment:** Enhance South Carolina industry's ability to effectively leverage cyber technical innovation emanating from NIWC Atlantic operations.*
- ***Attract:** Strengthen South Carolina's technical innovation landscape necessary to attract and retain cybersecurity talent, investment, and industry.*

The recent partnership between NIWC Atlantic/Palmetto Tech Bridge ("PTB") and SC Competes, via its Partnership Intermediary Agreement (PIA), will assist in driving industry growth by facilitating additional access to DoD-spurred technological innovations. This collaboration is key in simplifying the complex DoD technology transfer processes, making it easier for businesses to leverage advanced technologies for commercial use. By bridging the gap between military advancements and the commercial sector, this partnership not only promotes technological integration into the marketplace but also strengthens the competitive advantage of industries by providing them with high-grade tech solutions. We will address this priority through three mutually supportive lines of effort: growing the customer base, developing the workforce, and promoting public-private partnerships and investment opportunities.

First, we will expand the customer base by identifying and developing dual-use products and services that cater to both commercial interests and national security needs. Moving beyond a sole focus on the DoD, we will take affirmative steps to embrace a "whole of government" strategy, integrating a variety of stakeholders from both federal and state government agencies to yield substantial market growth for these technical solutions. Second, we will leverage the PIA activity to include a focus on developing a skilled workforce equipped to handle the challenges of the defense and cybersecurity industries, such as through joint training programs, workshops, and internships, thereby enhancing the skill sets of current employees while preparing new talent. Specifically, the developing historically black colleges and universities (HBCU) consortium will allow underrepresented students to access learning in a cohort-style setting as part of their cybersecurity skills training. And third, the partnership can facilitate public-private collaborations, attracting private investment into defense and cybersecurity projects. By creating an environment conducive to investment, we can spur innovation and economic growth. These partnerships can also lead to the development of new infrastructure, further bolstering South Carolina's position as a leader in these fields.

Key Partners: SC Council on Competitiveness, Palmetto Tech Bridge (NIWC Atlantic), SC Research Authority, Charleston Defense Contractors Association

Key Tasks:

- Facilitate collaboration between South Carolina industry and NIWC Atlantic to foster tech transfer initiatives.
- Identify opportunities for joint projects and initiatives that leverage technical innovation from NIWC Atlantic operations.

- Raise awareness among South Carolina industry stakeholders about the potential benefits of tech transfer from NIWC Atlantic.
- Educate industry partners about the available resources and opportunities for collaboration through initiatives like the Palmetto Tech Bridge.
- Provide guidance and support to South Carolina industry partners in navigating the complex processes involved in accessing DoD-spurred tech innovations.
- Assist industry partners in understanding and complying with DoD regulations and requirements for tech transfer.
- Engage with South Carolina industry associations, businesses, and stakeholders to solicit feedback and input on tech transfer priorities and needs.
- Foster dialogue and collaboration between industry and NIWC Atlantic to align tech transfer initiatives with industry growth objectives.
- Provide technical assistance and support to South Carolina industry partners in transferring and implementing DoD-spurred tech innovations into commercial products and solutions.
- Facilitate access to resources, expertise, and funding opportunities to support tech transfer initiatives.

Metrics of Performance:

- *Collaboration Facilitation*: Measure the number of collaborative initiatives facilitated between South Carolina industry and NIWC Atlantic to foster tech transfer.
- *Identification of Joint Projects*: Track the identification and initiation of joint projects and initiatives leveraging technical innovation from NIWC Atlantic operations.
- *Awareness-Raising Efforts*: Assess the effectiveness of raising awareness among South Carolina industry stakeholders about the potential benefits of tech transfer from NIWC Atlantic.
- *Education and Guidance*: Measure the provision of education and guidance to industry partners about available resources, collaboration opportunities, and processes for accessing DoD-spurred tech innovations.
- *Compliance Assistance*: Track the assistance provided to industry partners in understanding and complying with DoD regulations and requirements for tech transfer.
- *Engagement with Industry Associations*: Assess the level of engagement with South Carolina industry associations, businesses, and stakeholders to solicit feedback and input on tech transfer priorities and needs.
- *Dialogue and Collaboration Fostered*: Measure the extent of dialogue and collaboration fostered between industry and NIWC Atlantic to align tech transfer initiatives with industry growth objectives.
- *Technical Assistance Provided*: Track the provision of technical assistance and support to South Carolina industry partners in transferring and implementing DoD-spurred tech innovations into commercial products and solutions.
- *Access to Resources Facilitated*: Assess the facilitation of access to resources, expertise, and funding opportunities to support tech transfer initiatives.

Metrics of Effectiveness:

- *Number of Successful Tech Transfers*: Measure the number of successful tech transfers between NIWC Atlantic and South Carolina industry partners resulting in commercialized products or solutions.
- *Economic Impact*: Evaluate the economic impact of tech transfer initiatives on South Carolina's economy, including job creation, revenue generation, and industry growth.
- *Industry Growth and Innovation*: Assess the extent to which tech transfer initiatives contribute to industry growth and innovation in South Carolina.
- *Stakeholder Satisfaction*: Gather feedback from industry partners on their satisfaction with the support provided and the effectiveness of tech transfer initiatives.
- *Alignment with Industry Needs*: Evaluate the alignment of tech transfer initiatives with industry needs and priorities, as indicated by industry feedback and participation.
- *Long-Term Partnerships Established*: Measure the establishment of long-term partnerships and collaborations between NIWC Atlantic and South Carolina industry partners for ongoing tech transfer activities.

V. Innovation & Entrepreneurship

- **Making cybersecurity technical innovation accessible to South Carolina industry, academia, and government**
- **Making seed and growth capital accessible to cybersecurity entrepreneurs in South Carolina**

South Carolina has an enviable track record of growing and nurturing assets that create a vibrant landscape for technical innovation and entrepreneurial support within our legacy industry sectors. However, we must apply these strengths in a manner more tailored to the cybersecurity and broader information technology domain to keep pace with increasing digital transformation, automation, and interconnectedness across all facets of commerce and society.

IHEs, leading companies, federal partners, and non-profit force multipliers across South Carolina are making strides in cybersecurity technical innovation for manufacturing, transportation, port and maritime security, national defense, and more. We must ensure these efforts are properly resourced and championed in order to cultivate a coordinated ecosystem that appeals to cybersecurity researchers, entrepreneurs, executives, and investors looking for thriving innovation hubs where they can take their talents, passions, and resources.

14. Create Joint Appointments for SC Cybersecurity Faculty at SRNL

- ***Align:*** *Strengthen connectivity between South Carolina's academic research institutions and the resident national laboratory to foster increased collaboration across the cyber innovation landscape.*
- ***Augment:*** *Promote cyber technical innovation in South Carolina for increased access to cutting-edge cybersecurity applications.*
- ***Attract:*** *Foster a cyber innovation ecosystem that encourages and supports research and development, technology transfer, private investment, and entrepreneurship.*

Savannah River National Laboratory (SRNL), located in Aiken, SC, is one of only 17 national research & development laboratories under the US Department of Energy (DOE). Like other national labs, SRNL fosters collaboration with local and regional academic institutions through the use of joint appointments—positions in which university professors are partially appended to the Lab to strengthen its connectivity with other faculty, researchers, and students. Such positions help to grow innovation ecosystems surrounding joint research efforts, attracting additional participation and critical investment from the private sector. SRNL's main research areas include a rapidly growing focus on cybersecurity for national defense applications—but only one of the Lab's current joint appointees brings a cybersecurity focus, and he does not hail from a South Carolina academic institution.

We must create additional joint appointments at SRNL tied to universities in South Carolina—with a specific focus on cybersecurity research and development—to unlock further growth in our cyber ecosystem. Funds are available for appropriation to initiatives just like this one—to promote economic growth and critical infrastructure development in the Savannah River Site (SRS) area—as a result of the 2020 SRS Settlement with DOE, which saw the federal government dedicate $500M to the state of South Carolina. As our state's academic partners to SRNL, the University of South Carolina, South Carolina State University, and Clemson University would each benefit from state funding for a "Governor's Cyber Innovation Chair" or similarly titled position appended to the Lab. Including industry and non-profit leaders in selecting those joint appointees would help maximize the impact of the positions, ensuring that the successful candidates are poised to spur expanded collaboration across the wider cyber ecosystem. Of note, these dual appointments can be critical force multipliers to advance the objectives of the university-led programs included in strategic planning activity #17 below, which have the potential to garner more than $200M in additional federal funds for South Carolina's innovation ecosystem.

Key Partners: SC Office of the Governor, Savannah River National Laboratory, University of South Carolina, SC State University, Clemson University, SC Research Authority

Key Tasks:

- Explore interest for joint appointments at each university.
- Explore potential framework with the universities and SRNL, determine funding needs.
- Discuss potential for allocating SRS settlement funds with Office of the Governor
- Support legislation as required.
- Ensure cross-sector participation in helping universities to develop positional requirements and recruit and select candidates.

Metrics of Performance:

- *Discussion on Funding Allocation*: Track the discussions and progress made in exploring the potential allocation of SRS settlement funds with the Office of the Governor to support joint appointments.
- *Funding Secured*: Measure the success in securing the necessary funding for joint appointments through discussions with the Office of the Governor and potential alternative sources.
- *Cross-Sector Participation*: Measure the extent of cross-sector participation in helping universities develop positional requirements and recruit and select candidates for joint appointments.
- *Diversity of Candidates*: Evaluate the diversity and quality of candidates recruited for joint appointments, ensuring a broad and skilled pool of cybersecurity faculty.

Metrics of Effectiveness:

- *Growth of SRNL Cyber Innovation Partners*: Assess the growth of SRNL's cyber innovation network and strength of relationships therein.
- *Increased Cyber Collaboration across SRNL Innovation Network*: Assess the increase in SRNL's cyber-related innovation activity.
- *Increased Investor Engagement*: Assess the increase in investor interest and support to SRNL-affiliated cyber innovation activity.
- *Positive Impact on Cybersecurity Education*: Assess the impact of the joint appointments via increased ability to leverage SRNL assets, relationships, and support to benefit academic programming.

15. CATALYZE INVESTMENT IN SC CYBERSECURITY STARTUP AND GROWTH COMPANIES

- ***Align:*** *Address challenges impacting cyber entrepreneurs' ability to secure capital for business establishment and growth in South Carolina.*
- ***Augment:*** *Build upon the foundational business-friendly environment of South Carolina to more effectively address challenges facing cyber entrepreneurs.*
- ***Attract:*** *Position South Carolina as a compelling and supportive destination for cyber entrepreneurs and, in turn, cyber workers.*

The state of South Carolina recognizes the pressing need to accelerate investment in the cybersecurity sector to bolster its technical ecosystem and foster economic growth. We currently lack a robust pipeline of qualified cybersecurity companies for investment, and attracting private investment in this highly specialized field presents unique challenges. Investors must generate returns aligned with their investment thesis, and—absent cybersecurity expertise within investor groups—it is challenging for them to pursue opportunities in the cyber sector without considerable incentives and risk reduction. As a result, there is an inherent disconnect between investors' fiduciary responsibilities and the state's economic development goals in the cyber sector—both for incubating startups and supporting companies through growth.

To address the identified challenges and capitalize on the growing importance of cybersecurity for economically thriving and secure states, we recommend the creation of two separate funds: a $25M venture studio fund for cyber startups, and a $150M growth equity fund for cyber growth companies. The venture fund would focus on nurturing and incubating cyber startups within South Carolina by offering financial support, mentorship, co-working spaces, and access to resources that can attract promising cyber companies to the state and help them develop. Meanwhile, the growth equity fund would focus on supporting established cyber companies seeking to relocate or expand to establish a significant presence in South Carolina. This fund should be prepared to allocate larger monies, as the growth and expansion of cyber firms often require substantial capital, and to collaborate with institutional investors and growth equity partners to secure the necessary funding for larger investments.

These two funds will work in tandem to address the limited cybersecurity investment pipeline, provide support to both early-stage and growth-stage companies, and remove conflicts of interest among investors. By adopting this strategy, South Carolina can position itself as a cybersecurity destination, stimulate economic growth, and strengthen its cybersecurity defenses, ultimately benefiting both investors and the state's long-term economic goals.

Key Partners: SC Research Authority, SC Department of Commerce, InvestSC

Key Tasks:

- Establish a $25M venture studio fund for cybersecurity startups.
- Establish a $150M growth equity fund for cybersecurity growth companies.
- Develop clear and comprehensive criteria for selecting cybersecurity startups and growth companies for investment.

- Implement strategies to identify and attract qualified cybersecurity startups and growth companies to South Carolina.
- Engage with potential investors, including institutional investors and growth equity partners.
- Communicate the investment thesis and benefits of investing in the South Carolina cybersecurity sector.
- Develop mechanisms to mitigate risks for investors lacking cybersecurity expertise.
- Implement incentives to attract investors and align their interests with the state's economic development goals.
- Strategically allocate funds to support the specific needs of early-stage startups and growth-stage companies.
- Collaborate with government agencies, industry associations, and educational institutions to create a supportive ecosystem for cybersecurity companies.
- Establish mentorship programs for cybersecurity startups.
- Provide co-working spaces and access to resources to facilitate the development of startups.
- Conduct thorough due diligence on potential investment opportunities to ensure alignment with fund objectives.
- Develop a marketing strategy to promote South Carolina as a cybersecurity destination.
- Highlight success stories and the impact of investments on economic growth.

Metrics of Performance:

- *Establishment of Venture Studio Fund*: Measure the successful establishment of the $25M venture studio fund for cybersecurity startups.
- *Establishment of Growth Equity Fund*: Assess the successful establishment of the $150M growth equity fund for cybersecurity growth companies.
- *Development of Investment Criteria*: Track the development of clear and comprehensive criteria for selecting cybersecurity startups and growth companies for investment.
- *Implementation of Startup and Growth Company Strategies*: Evaluate the effectiveness of implemented strategies to identify and attract qualified cybersecurity startups and growth companies to South Carolina.
- *Engagement with Potential Investors*: Measure the engagement level with potential investors, including institutional investors and growth equity partners.
- *Communication of Investment Thesis*: Assess the success in communicating the investment thesis and benefits of investing in the South Carolina cybersecurity sector.
- *Development of Risk Mitigation Mechanisms*: Track the development and implementation of mechanisms to mitigate risks for investors lacking cybersecurity expertise.
- *Implementation of Investor Incentives*: Evaluate the successful implementation of incentives to attract investors and align their interests with the state's economic development goals.

- *Strategic Allocation of Funds*: Measure the effectiveness of strategically allocating funds to support the specific needs of early-stage startups and growth-stage companies.

Metrics of Effectiveness:

- *Number of Funded Startups and Growth of Companies*: Assess the effectiveness of the initiative by measuring the number of cybersecurity startups and growth of companies funded through the established funds.
- *Job Creation*: Evaluate the impact on job creation in the cybersecurity sector as a result of investments, considering both direct and indirect employment.
- *Diversity of Funded Companies*: Measure the diversity of the funded cybersecurity startups and growth companies, considering factors such as size, industry focus, and ownership.
- *Economic Growth in the Cybersecurity Sector*: Assess the overall economic growth and development in the cybersecurity sector of South Carolina resulting from the investments.
- *Investor Satisfaction*: Gather feedback from investors to assess their satisfaction with the investment process, communication, and outcomes.
- *Alignment with Economic Development Goals*: Evaluate the extent to which investor interests align with the state's economic development goals.
- *Long-Term Viability of Funded Companies*: Measure the long-term viability and success of cybersecurity startups and growth companies funded through the initiative.

16. Develop a Mentor Network for Cybersecurity Entrepreneurs

- ***Align:*** *Consolidate South Carolina's resident expertise in cybersecurity business formation and growth to support cyber entrepreneurs more effectively.*
- ***Augment:*** *Improve conditions for cyber companies to establish and grow in South Carolina, strengthening our technical ecosystem, growing job opportunities, and fostering economic growth.*
- ***Attract:*** *Position South Carolina as a supportive home for cyber entrepreneurship and investment.*

One critical ingredient for successful entrepreneurship—especially in a field as complex and dynamic as cybersecurity—is mentorship. For cybersecurity entrepreneurs in South Carolina, having access to experienced mentors can be transformative. These mentors provide not only technical guidance but also insights into business strategy, funding, and networking. They can help navigate the unique challenges of the cybersecurity industry, from understanding regulatory landscapes to identifying emerging market trends. Moreover, mentorship can significantly shorten the learning curve for new entrepreneurs. It offers a blend of personalized advice, practical experience, and industry connections that are invaluable for building viable commercial enterprises. In turn, these companies can not only attract significant investment, create high-value jobs, and stimulate technical advancements, but also address cybersecurity challenges worldwide—expanding the global market for South Carolina industry.

To promote the growth of this impactful industry, we must build a mentorship program for cyber entrepreneurs that offers scalable support to businesses at various stages of maturity. For market entrants, the program can provide group classes on business basics and facilitate networking opportunities to help entrepreneurs leverage additional resources. These services may be best delivered virtually, to enable cost efficiency and flexible learning and engagement. The next level of support would involve more tailored workshops to help scope service and product offerings, explore market opportunities, and develop marketing strategies. At the other end of the spectrum, entrepreneurs can access personalized mentoring specific to their business needs and challenges, to include scaling and/or refining their business models and technical offerings. In addition to helping cyber business leaders, these mentors can also play a key role in aligning industry growth with the state's economic development goals, investment landscape, talent development, and innovation activities—serving as a critical "connective tissue" between the private sector and this wider range of cyber ecosystem assets and initiatives.

Such a program will require dedicated resources and must be positioned to effectively liaise among and advocate for the equities of entrepreneurs and other ecosystem stakeholders alike. As such, an organization like the SC Research Authority or the SC Department of Commerce would serve as an ideal home for this activity, both for realizing programmatic efficiencies and for leveraging existing public-private stakeholder networks.

Key Partners: SC Research Authority, SC Department of Commerce, SC Small Business Development Centers; entrepreneurial support organizations (e.g., NextGEN, Harbor Entrepreneur Center, Boyd Innovation Center)

Key Tasks:

- Define the structure and objectives of the mentor network program, considering the needs of cybersecurity entrepreneurs at various stages of business maturity.
- Identify experienced professionals in the cybersecurity industry who are willing to serve as mentors. Assess their expertise, availability, and willingness to provide guidance to entrepreneurs.
- Develop a system for matching mentors with mentees based on their needs, industry focus, and business stage.
- Provide training and orientation sessions for both mentors and mentees to ensure they understand their roles and responsibilities within the program.
- Develop educational materials, templates, and resources to support mentorship activities, covering topics such as business strategy, funding, regulatory compliance, and market trends.
- Organize networking events, workshops, and seminars to facilitate connections between mentors, mentees, and other stakeholders in the cybersecurity ecosystem.
- Establish mechanisms for gathering feedback from participants to continuously improve the mentor network program. Conduct periodic evaluations to measure the effectiveness and impact of the program on the growth and success of cybersecurity entrepreneurs.
- Implement virtual delivery mechanisms for mentorship activities to maximize accessibility and cost efficiency for participants.

- Develop a marketing and outreach strategy to promote awareness of the mentor network program among cybersecurity entrepreneurs and potential mentors.
- Establish a dedicated team or organization responsible for managing and coordinating the mentor network program, including logistics, communication, and administration.

Metrics of Performance:

- *Program Design and Development*: Completion of the definition of the structure and objectives of the mentor network program.
- *Identification of Mentor Candidates*: Number of experienced professionals in the cybersecurity industry identified and assessed for their suitability as mentors.
- *Matchmaking Success*: Percentage of mentors successfully matched with mentees based on their needs, industry focus, and business stage.
- *Training and Orientation Completion*: Percentage of mentors and mentees who complete training and orientation sessions to understand their roles and responsibilities.
- *Resource Development*: Completion of educational materials, templates, and resources to support mentorship activities.
- *Networking Event Organization*: Number of networking events, workshops, and seminars organized to facilitate connections between mentors, mentees, and stakeholders.
- *Virtual Delivery Implementation*: Successful implementation of virtual delivery mechanisms for mentorship activities.
- *Program Promotion*: Effectiveness of the marketing and outreach strategy in promoting awareness of the mentor network program among cybersecurity entrepreneurs and potential mentors.
- *Program Management Establishment*: Establishment of a dedicated team or organization responsible for managing and coordinating the mentor network program.

Metrics of Effectiveness:

- *Participant Satisfaction*: Gather feedback from mentors and mentees to assess satisfaction with the mentorship program and its impact on their growth and success.
- *Number of Successful Mentorships*: Measure the number of successful mentorships established through the program, leading to tangible outcomes such as business growth, funding, or market expansion.
- *Business Growth of Mentees*: Assess the growth and success of mentee businesses over time, including factors such as revenue growth, market share, and customer acquisition.
- *Networking and Collaboration Opportunities*: Evaluate the extent to which participants leverage networking events and collaborations facilitated by the mentor network program to advance their businesses.

- *Feedback Utilization*: Utilize feedback gathered from participants to continuously improve and refine the mentor network program, addressing any identified shortcomings or areas for enhancement.
- *Long-Term Sustainability*: Measure the long-term sustainability of the mentor network program, including its ability to maintain participant engagement and support entrepreneurship in the cybersecurity sector over time.

17. SUPPORT SC UNIVERSITY-LED, FEDERALLY FUNDED CYBER INNOVATION PROGRAMS

- ***Align:*** *Promote effective collaboration across South Carolina's assets for cyber innovation, education, workforce development, industry, and posture & readiness.*
- ***Augment:*** *Bolster the success of South Carolina's cyber innovation programs and increase their ability to secure additional federal and other funds for continued technical and economic development.*
- ***Attract:*** *Accelerate the transformation of South Carolina's cyber innovation ecosystem to more effectively compete for industry, workforce, and investment resources.*

Our state is home to two nascent, but critical, initiatives designed to spur technical cybersecurity innovation through increased collaboration across a wide range of stakeholders. These programs—both the recipients of federal grant funds as a result of nationwide competitions—stand poised to transform South Carolina's cyber innovation landscape and secure additional resources for the state's continued technical and economic growth.

The South Carolina Maritime Cybersecurity Regional Innovation Engine, led by the University of South Carolina Beaufort (USCB), was awarded a two-year, $1M planning grant from the National Science Foundation (NSF) in 2023. This activity aims to conduct research to better understand the interdependencies, vulnerabilities, and risks within the maritime transportation ecosystem and develop solutions using artificial intelligence, machine learning, and blockchain technologies to maximize efficient and effective cybersecurity defense. With a geographic focus area encompassing the Ports of Charleston and Georgetown, the Jasper Ocean Terminal project, and the truck and rail system serving those ports (including the Inland Ports of Greer and Dillon), the innovation engine will address cybersecurity workforce development (specific to the maritime transportation system); technical research and development; and economic development through new business creation and investment. USCB and its partners across the state—including universities, technical colleges, industry associations, non-profits, and state and federal agencies—are currently applying for an additional $160M in NSF funding over the next ten years to implement the plans and transform South Carolina's cyber innovation landscape.

The National Center for Transportation Cybersecurity and Resiliency (TraCR), established at Clemson University in 2023 through funding from the US Department of Transportation (USDOT), is focused on building an iron-clad defense against cyberattacks on the nation's transportation systems by pioneering advanced security strategies and technical solutions. TraCR and its academic partners in South Carolina will develop specialized transportation cybersecurity courses and lead outreach efforts to grow the requisite workforce pipeline; design a national platform for conducting vulnerability assessments on transportation infrastructure; and conduct research in four key areas (security and resiliency, user and data privacy, society and environment, and quantum computing) to guide technical solutions development. In order to secure a continued federal investment of $1.45M per year from the USDOT, TraCR must demonstrate an annual match of $1.45M from non-federal sources.

These two programs combine to form a unique opportunity for South Carolina to accelerate its cyber research and development output; increase collaboration across the breadth of its resident cyber stakeholders; and position itself as a leading hub for cybersecurity innovation. To unlock their transformative potential, we must ensure they are adequately championed, supported, and resourced—to include via direct state investment.

Key Partners: University of South Carolina Beaufort, Clemson University, SC Research Authority, SC Council on Competitiveness, SC Office of the Governor, SC Department of Commerce, SC Ports Authority

Key Tasks:

- Convene Innovation Engine and TraCR principals with SCRA, SC Commerce and Governor's Office to promote awareness and pursue state investment.
- Establish timing and mechanism for recurring check-ins with the above entities to stay apprised of risks to program success and explore state assistance to manage risks.
- Ensure both activities are represented on the state's centralized cyber portal and effectively marketed to garner increased engagement and support.

Metrics of Performance:

- *Convening of Principals*: Measure the successful convening of Innovation Engine and TraCR principals with SCRA, SC Commerce, and the Governor's Office to promote awareness and pursue state investment.
- *Establishment of Recurring Check-ins*: Track the establishment of timing and mechanism for recurring check-ins with relevant entities to stay apprised of risks to program success and explore state assistance to manage risks.
- *Representation on Cyber Portal*: Assess whether both activities are represented on the state's centralized cyber portal, ensuring visibility, and accessibility to stakeholders.
- *Marketing Effectiveness*: Measure the effectiveness of marketing efforts to garner increased engagement and support for the grant programs.

Metrics of Effectiveness:

- *Awareness and Engagement*: Evaluate the level of awareness and engagement among stakeholders, including universities, government entities, and potential grant applicants, regarding the grant programs.
- *State Investment Secured*: Assess whether state investment is secured for the federally funded programs as a result of the efforts to promote awareness and explore investment opportunities. Measure the effectiveness of the established check-ins in identifying and managing risks to program success, ensuring smooth operation and delivery of programs.

- *Increased Support and Participation*: Track any increase in support and participation in the programs, indicating the success of marketing efforts in garnering increased engagement.
- *Program Success Stories*: Document and highlight success stories and outcomes from the programs, showcasing the impact of state support and investment in fostering cyber innovation at universities.
- *Feedback from Stakeholders*: Gather feedback from stakeholders on the effectiveness of the support provided and the overall success of the programs in promoting cyber innovation.
- *Alignment with State Goals*: Evaluate the extent to which the programs align with state goals and priorities in advancing cyber innovation and economic development.
- *Long-Term Sustainability*: Assess the long-term sustainability of the programs and their ability to continue fostering cyber innovation at universities beyond the initial support period.

VI. Defense Partnerships

- **Making a cyber-ready workforce and enabling asset environment accessible to state and regional DoD missions**
- **Making high-growth cyber career opportunities accessible to South Carolina's separating servicemembers and veterans**

The Department of Defense (DoD) serves as an outsized source of cybersecurity talent and demand for cybersecurity services in South Carolina, with numerous critical cyber missions located within and adjacent to our state. From major tenants like Naval Information Warfare Center (NIWC) Atlantic, Shaw Air Force Base, and the SC National Guard's 125th Cyber Protection Battalion, to neighboring military cyber command units at Fort Eisenhower, Georgia, our local defense elements offer unparalleled cyber expertise. Their efforts to preserve national security and maintain America's competitive advantage against foreign adversaries requires the full support of our ecosystem. We must develop a sustainable, local cybersecurity workforce that can support these missions, backed by a vibrant cyber industry and innovation landscape.

South Carolina's commitment to our defense assets does not end with supporting active missions, however. We must continue to provide every opportunity to separating servicemembers and veterans to successfully compete for fulfilling jobs following their military service—to include in the high-demand, high-earnings field of cybersecurity. We must also create opportunities for servicemembers to help educate and support South Carolina residents and organizations in enhancing their cybersecurity posture and readiness. By improving connectivity between defense, industry, and academic partners we can increasingly facilitate career transition, knowledge exchange, and resource sharing for collective benefit.

18. INCREASE SC CYBER EMPLOYER PARTICIPATION IN DOD SKILLBRIDGE PROGRAM

- ***Align:*** *Strengthen connectivity between separating servicemember pipeline and cybersecurity employers in South Carolina.*
- ***Augment:*** *Grow South Carolina's cybersecurity workforce while improving job opportunities for proven performers from our nation's military.*
- ***Attract:*** *Retain veteran talent within South Carolina and facilitate their transition to post-military careers.*

South Carolina is committed to helping the members of our armed forces successfully transition to meaningful and rewarding civilian careers following their military service. Such a move is not always easy, as entering the private sector (or non-military public sector) requires navigating entirely new networks, processes, and communications styles. Fortunately, a DoD program designed to assist with this transition is being leveraged by employers and separating servicemembers in our state—but we have ample room to increase its usage for cybersecurity positions in particular.

The DoD SkillBridge program is a nationwide platform for connecting servicemembers who are about to leave active duty with civilian job opportunities where they can gain critical experience and on-the-job training to successfully pursue post-service employment. To register with SkillBridge, participating employers must develop a structured training program and demonstrate their readiness to properly integrate and support servicemembers through internships, apprenticeships, or other work-training opportunities. Meanwhile, with their unit commander's approval, participating servicemembers can be released from their military duties for up to the final 180 days of their active service to work and train with an approved SkillBridge employer. Importantly, the servicemember continues to receive their full military pay and benefits during this engagement—enabling them to develop job skills and gain work experience while the employer benefits from their talents and develops their workforce at no additional cost.

While South Carolina is home to over 170 registered SkillBridge employer programs, only six involve cybersecurity, representing a significant untapped potential. With our state needing to attract and/or grow nearly 6,000 additional cyber workers in the next 10 years to meet forecasted demand—and in light of our proximity to multiple DoD installations with heavy concentrations of cybersecurity-savvy servicemembers—we must increase our cyber employers' use of this program. From a focused campaign to raise employer awareness of SkillBridge and its value, to direct assistance and "playbooks" for developing required training programs and complying with registration requirements, to promoting unit commander "buy-in" and resolving the challenges of authorizing mission absence, we must work to better connect the two ends of this critical workforce pipeline. Because servicemembers can participate in SkillBridge programs outside of their assigned duty areas, we can also actively market SC-based programs to select military installations across the US that have high concentrations of cyber personnel and create a regional "landing pad" to attract remote servicemembers and provide logistical support. An increased investment in DoD SkillBridge is an investment in our state's cyber industry and workforce, in our information security and privacy, and in the lives of the men and women who have served in our armed forces.

Key Partners: SC Department of Veterans Affairs, SC Department of Commerce, unit commanders and transition assistance program (TAP) officials at NIWC Atlantic, Shaw AFB, MCAS Beaufort, MCRD Parris Island, and Fort Eisenhower

Key Tasks:

- Engage DoD SkillBridge program representative to understand employer registration requirements and training criteria.
- Engage cyber unit commanders and TAP officials at local military installations to develop solutions to constraints on authorizing servicemember participation.
- Develop communications materials and processes for marketing SkillBridge value to SC cyber employers.
- Emplace resources for assisting SC cyber companies with SkillBridge program registration and development.

Metrics of Performance:

- *Engagement with DoD SkillBridge Program Representative*: Measure the successful engagement with DoD SkillBridge program representatives to understand employer registration requirements and training criteria.

- *Engagement with Unit Commanders and TAP Officials*: Track the level of engagement with unit commanders and Transition Assistance Program (TAP) officials at local military installations to develop solutions to constraints on authorizing servicemember participation.
- *Development of Communications Materials*: Measure the completion of communication materials and processes for marketing the value of the SkillBridge program to SC cyber employers.
- *Emplacement of Resources for Assistance*: Track the establishment of resources aimed at assisting SC cyber companies with SkillBridge program registration and development.

Metrics of Effectiveness:

- *Increase in Employer Participation*: Measure the increase in the number of SC cyber employers participating in the DoD SkillBridge program.
- *Number of Solutions Developed*: Assess the number of solutions developed with cyber unit commanders and TAP officials to address constraints on authorizing servicemember participation.
- *Employer Satisfaction*: Gather feedback from SC cyber employers to assess their satisfaction with the assistance provided and the effectiveness of the program in meeting their needs.
- *Number of Registered Companies*: Measure the number of SC cyber companies registered for the SkillBridge program after receiving assistance and marketing efforts.
- *Servicemember Participation Rates*: Track the increase in the number of servicemembers from SC participating in SkillBridge training programs with cyber employers.
- *Program Awareness*: Evaluate the awareness of the SkillBridge program among SC cyber employers and the broader cybersecurity community in the state.
- *Impact on Transition Success*: Assess the impact of increased employer participation in the SkillBridge program on the successful transition of servicemembers to civilian careers in cybersecurity.

19. ESTABLISH ACCELERATED TRAINING PROGRAM TO SUPPORT DOD CYBER MISSIONS

- ***Align:*** *Build a tailored asset to efficiently address DoD cyber workforce shortfalls while also further developing South Carolina's cyber education and workforce development landscape.*
- ***Augment:*** *Boost DoD's ability to carry out its cybersecurity missions most effectively in the furtherance of national security.*
- ***Attract:*** *Establish South Carolina as a leader in innovative cyber education and workforce development programs while enabling the state to serve as a workforce magnet.*

Just as state and local governments face difficulties in addressing their cyber workforce needs, the Department of Defense is challenged to fill every cybersecurity position required to fully prosecute its national security missions. Given our state's proximity to multiple DoD bases with robust cybersecurity activities, South Carolina (and our region at large) is home to a large collection of DoD contract companies that compete to hire qualified cyber workers who can be placed on these federal contracts—but unfilled billets continue to impede mission performance. A major driver of this worker supply challenge is that these contract billets require a specific combination of skills and certifications tailored to DoD requirements—so how can we increase the supply of qualified workers? The blueprint for a solution may lie in a program that has successfully addressed a similar workforce challenge affecting the shipbuilding industry for the US Navy.

The Accelerated Training in Defense Manufacturing (ATDM) program, located in Danville, VA, and spearheaded by the Institute for Advanced Learning and Research (IALR), was created several years ago with funding from the DoD's Industrial Base Analysis and Sustainment (IBAS) program. ATDM addresses critical workforce shortages in DoD's shipbuilding industry tied to specific technical capabilities (such as additive manufacturing and CNC machining). Participants need not have any specific work experience or technical skills—the training is designed to progress students from "zero" to "DoD-certified" in four months (eight hours a day, five days a week). And while veterans and even active-duty servicemembers (via the DoD SkillBridge program) can participate, the training is not specifically geared towards them—graduates are intended for the defense industrial base, not necessarily from DoD. The program covers the costs of training, housing, and transportation, while students must cover their own costs for food and other typical expenses. In addition to the technical training and certifications, students also receive job placement and relocation assistance, as ATDM serves a critical connective role between this workforce source and the contract companies across the country who employ its graduates. As a result of the program's success, ATDM recently broke ground for a new, expanded training facility in Danville, and IALR (and its partners, including Danville Community College and the Phillips Corporation) have surrounded ATDM with a host of supporting academic, workforce development, and R&D assets to comprise a budding innovation hub.

Whether funding can be secured from DoD IBAS to develop a cybersecurity equivalent in our state or whether South Carolina government, industry, and academia can partner to invest in such an asset, the value proposition is arguably stronger than that of the now-proven ATDM concept. First, while shipbuilding is certainly a central component of our nation's defense, the criticality of cybersecurity is increasing exponentially, it impacts every facet of our society, and its economic impact cannot be overstated. Second, the success of such a program is contingent upon a nationwide audience being willing to relocate (potentially with their families) to the training facility's geography—and with South Carolina's recognized quality of life and resident hospitality industry, we do not face the same uphill battle that Danville did. Third, our state already hosts a strong array of supporting assets, programs, initiatives, and networks critical to ensuring the rapid set-up and sustained success of such a program—we would not be starting from scratch. An accelerated cyber training program—perhaps tied to the USC Beaufort-led Innovation Engine program, both to take advantage of the Lowcountry's tourism readiness and to leverage the NSF-funded cybersecurity growth there—would put South Carolina on the national map as a cyber workforce innovator, turbocharge DoD's ability to secure the cyber talent it needs, and emplace a key asset for strengthening DoD-industry-academia collaboration in our region.

Key Partners: SC Department of Veterans Affairs, South Coast Cyber Center, University of South Carolina Beaufort, Technical College of the Lowcountry, The Citadel, Charleston Defense Contractors Association, the Alliance for Fort Eisenhower, SC Department of Employment and Workforce

Key Tasks:

- Engage CDCA to understand skills and certifications requirements for DoD cyber contract billets and impact to necessary training outcomes
- Determine how "accelerated" cyber training could be if applied 40 hours per week, in order to meet established DoD contract workforce qualifications
- Engage DoD IBAS to explore potential federal funding, in conjunction with engaging ATDM to explore pitfalls and lessons learned
- Engage Beaufort-area cyber stakeholders to explore feasibility of logistics
- Engage state government and industry to identify additional sources of sponsorship, funding, and sustainment

Metrics of Performance:

- *Understanding Requirements*: Measure successful engagement with the CDCA, prime cyber contract companies, and/or DoD contract managers to understand skills and certifications requirements for DoD cyber contract billets.
- *Determination of Accelerated Training Duration*: Track the determination of how "accelerated" cyber training could be if applied 40 hours per week to meet established DoD contract workforce qualifications.
- *Engagement with DoD IBAS and ATDM*: Measure the engagement with the DoD IBAS and ATDM to explore potential federal funding and pitfalls/lessons learned, respectively.
- *Engagement with Beaufort-area Cyber Stakeholders*: Assess the level of engagement with Beaufort-area cyber stakeholders to explore the feasibility of logistics for the training program.
- *Engagement with State Government and Industry*: Measure the engagement with state government and industry to identify additional sources of sponsorship, funding, and sustainment for the training program.

Metrics of Effectiveness:

- *Development of Training Program Framework*: Evaluate the development of a comprehensive framework for the accelerated training program, including curricula, training outcomes, and scheduling.
- *Alignment with DoD Contract Workforce Qualifications*: Assess the extent to which the accelerated training program aligns with established DoD contract workforce qualifications and requirements.
- *Availability of Federal Funding*: Measure the availability and utilization of federal funding secured through engagement with DoD IBAS and exploration of potential funding sources.

- *Feasibility Assessment*: Evaluate the feasibility of logistics in the Beaufort area for implementing the accelerated training program, considering factors such as infrastructure, facilities, and transportation.
- *Sponsorship and Funding Sources Identified*: Track the identification of additional sources of sponsorship, funding, and sustainment for the training program, including commitments from state government and industry partners.
- *Number of Participants Enrolled*: Measure the number of participants enrolled in the accelerated training program, indicating the level of interest and demand.
- *Success Rate of Graduates*: Assess the success rate of graduates from the accelerated training program in obtaining DoD cyber contract billets or related positions, indicating the effectiveness of the program in meeting its objectives.
- *Long-Term Sustainability*: Evaluate the long-term sustainability of the training program, including its ability to continue providing training and support for future DoD cyber missions.

20. AMPLIFY AIKEN / NORTH AUGUSTA REGIONAL CYBER ECOSYSTEM DEVELOPMENT EFFORTS

- ***Align:*** *Ensure resources are optimized to maximize South Carolina's ability to support national defense and realize economic gains associated with Fort Eisenhower's cybersecurity mission and broader regional innovation.*
- ***Augment:*** *Bolster the success of North Augusta- and Aiken-area initiatives to attract and grow cyber companies, workforce, innovation assets, and investment.*
- ***Attract:*** *Demonstrate South Carolina's commitment to creating favorable conditions for cyber companies and workers to thrive while supporting critical cyber defense missions.*

Cybersecurity's role within and criticality to the security of our nation continues to grow. As directed in the National Defense Authorization Act for Fiscal Year 2023, the DoD established the Assistant Secretary of Defense for Cyber Policy (ASD(CP)) for overall supervision of DoD policy for cyber operations. Accordingly, DoD cyber growth has led to a continual expansion of operations and resource needs at Fort Eisenhower, GA, over the last decade, resulting in an increasing array of opportunities for South Carolina to support national defense missions and explore related avenues for economic growth.

In response, regional stakeholders have grown key initiatives and assets to maximize these opportunities. The Alliance for Fort Eisenhower works to ensure that the Central Savannah River Area (CSRA) gains widespread recognition as a competitive district for cyber work, research, and innovation. The Georgia Cyber Center has continued to expand as it fosters collaboration among government, academia, and industry. And here in South Carolina, supporting efforts have been established among partners including the Savannah River National Laboratory (SRNL), the University of South Carolina Aiken, the South Carolina National Guard, and municipal leaders in Aiken and North Augusta.

As one example, the future National Guard Cyber Innovation Center is a partnership between the South Carolina National Guard and USC Aiken to create a $13M Cyber Integration Center, including a SCIF, to provide connectivity to Fort Eisenhower, enhance cybersecurity initiatives, and attract industry to South Carolina. The state-of-the-art center, slated for land adjacent to SRNL's Advanced Manufacturing Collaborative (AMC) on the university's campus, will serve as an ecosystem for cyber experts in private, government, and academic sectors and include space for classes, training areas, and operational and administrative suites. The campus will also house a separate $31M National Guard Cyber "Readiness Center," supporting training and logistics for three cyber and signal units and providing USC Aiken students with mentorship opportunities and real-world experience. Meanwhile, the AMC itself will serve as an innovation hub for manufacturing, fostering modern industrial practices, advancing new technologies, and training the future manufacturing workforce with a focus on chemical and materials manufacturing. The AMC is a true public-private partnership, combining the unique capabilities of the US Department of Energy's (DOE) National Laboratories, industrial enterprises, and educational institutions to drive long-term sustainability of the US manufacturing sector—already a critical component of South Carolina's industry landscape.

There is extraordinary potential for the Aiken region to further benefit from the growth opportunities offered by Fort Eisenhower-driven cyber expansion—whether positioning the area as a competitive home for cyber industry; developing additional assets to support federal and state innovation activity; or advancing educational and work opportunities to support military and civilian cyber workers and their families. We must ensure that state resources and attention are appropriately positioned to support this regional growth.

Key Partners: SC Department of Commerce, county and municipal leadership, SC Department of Veterans' Affairs, SC Department of Transportation, Savannah River National Laboratory, South Carolina National Guard, USC Aiken

Key Tasks:

- Leverage the Key Partners to foster and strengthen strong relations at Fort Eisenhower.
- Assist cyber and signal soldiers transitioning from active duty at Fort Eisenhower to continue service in the military's Reserve and Guard components as they pursue civilian careers.
- Support cybersecurity initiatives in South Carolina sponsored by The Alliance for Fort Eisenhower.
- Promote awareness of regional growth while documenting and highlighting success stories and lessons learned.

Metrics of Performance:

- *Increase Understanding of Fort Eisenhower Mission Requirements*: Continually assess Fort Eisenhower's current and future mission sets which are currently under-resourced and translate those requirements into terminology that can be easily understood by government officials, economic developers, academic leaders, and industry executives.
- *Increase Understanding of Cybersecurity Company and Workforce Needs:* Assess what inhibitors (real and perceived) exist for companies to establish operations in the Aiken area and for workers/families to locate there, and what incentives may need to be offered.

Metrics of Effectiveness:

- *Target Audiences Investing in the Aiken Region*: Assess the number and scope of businesses, investors, and workforce talent relocating to the area in order to support resident and nearby cybersecurity missions and assets.
- *Growth of Cyber-Driven Economic Impact*: Assess the increase in regional economic growth attributable to cybersecurity-related workforce and commercial growth.

VII. Acknowledgments

This strategic plan was developed by Simon Everett, Ltd., via a contract with WesternSC in partnership with the SC Department of Commerce.

The plan was developed through the efforts of five working groups—one for each pillar—that were convened to solicit the insights of a wide range of stakeholders across South Carolina who have equities in a given pillar. "Cross-pollination" of stakeholders was intentional, e.g., representatives of educational institutions were not confined to the education & workforce development working group. These groups discussed potential initiatives that originated from the preceding ecosystem study; ideated additional initiatives for consideration; explored pathways forward and key challenges; and—in some cases where an initiative lay within a stakeholder's existing scope of responsibility—began implementing initial steps. The initiatives presented herein were informed not only by those working group meetings, but also by dozens of targeted exchanges among subsets of stakeholders.

The members of each working group are listed below, and we thank them for contributing their time and expertise towards helping South Carolina improve its cybersecurity ecosystem. The leads of each working group are listed first, in bold. Members' organizational affiliations reflect their time of supporting the working groups; some have since changed.

EDUCATION & WORKFORCE DEVELOPMENT

Nina Staggers, SC Department of Employment and Workforce
Claire Allen, Mantech
Dr. Shankar Banik, The Citadel
Melanie Barton, SC Office of the Governor
Dr. Bob Couch, Anderson School District 5
Benjamin Dusek, SC Department of Education
Sally Ehrenfried, Blackbaud
Patricia Ferguson, SC Department of Commerce
Brenda Gardner, SC Department of Employment and Workforce
Ricky Gaylard, ISC2 Chapter, Charleston
Chad Hardaway, USC Columbia, Office of Economic Engagement
Angel Kern, Technical College of the Lowcountry
Lelia King, Build Carolina
Debbie McLeod, McLeod Information Systems
Dr. Rudy (Rusty) Monhollon, SC Commission on Higher Education
Qunicie Moore, SC Department of Education
Ian O'Briant, Check Point Software Technologies
Mauricio Orozco, ISC2 Chapter, Midlands
Amanda Richardson, Apprenticeship Carolina
Dr. Frank Rodriguez, Beaufort County School District
Rosaline Sumpter, SC Technical College System
Dr. Nikunja Swain, SC State University
Dr. Kuang-Ching (KC) Wang, Clemson University

POSTURE & READINESS

Mark Plowden, SC Office of the Governor
Alex Alvanos, SC Department of Administration
CL Clay, Cybersecurity and Infrastructure Security Agency
Sean Fay, SC Department of Social Services
Joe Greer, Capgemini Advanced Technology Development Center
Earl Gregorich, SC Small Business Development Centers
Roger Hall, SC Department of Consumer Affairs
Sarah Hines, SC Small Business Development Centers
Paul Ihme, Soteria
Lindsey Kremlick, SC Department of Administration
M. Kent Lesesne, SC Association of Counties
Mark Lester, SC Ports Authority
Bailey Parker, SC Department of Consumer Affairs
Ryan Truskey, SC Critical Infrastructure Cybersecurity (CIC) Program
Frank Waszmer, Prisma Health
Erica Wright, Municipal Association of SC

INDUSTRY GROWTH

Susie Shannon, SC Council on Competitiveness
Megan Anderson, Charleston Regional Development Alliance
Dr. Laurie Boeding, Trident Technical College
Jim Clifford, City of North Augusta
Jeffrey DeLung, North Eastern Strategic Alliance
Christopher Finn, I-77 Alliance
Dr. Joseph Fitsanakis, Coastal Carolina University
Dr. Rebecca Gunnlaugsson, SC Department of Commerce
Tracy McMillin, Central SC Alliance
Brad Neese, readySC // South Carolina Technical College System
Brian Rauschenbach, The LINK Economic Alliance
Sandy Steele, SC Regional Development Alliance // SC Economic Developers' Association
Elizabeth Watson, Upstate SC Alliance
Will Williams, WesternSC

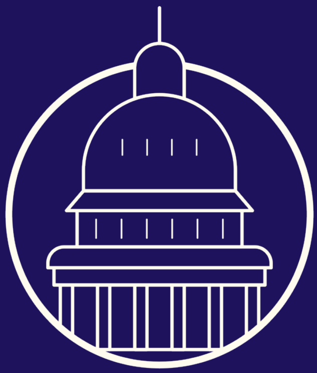
INNOVATION & ENTREPRENEURSHIP

Bob Quinn, SC Research Authority
Adam Anderson, Hook Security
Ernest Andrade, Charleston Digital Corridor
Charlie Banks, VentureSouth
Nathaniel Barber, SC Community Loan Fund
Wiley Becker, Alerion Ventures
Suzanne Dickerson, Director of SC Fraunhofer USA Alliance, SC Council on Competitiveness
Dr. Ethan Farquhar, Savannah River National Laboratory
Robby Hill, HillSouth
Shaler Houser, Deal Strategies
Bill Kirkland, USC Columbia, Office of Economic Engagement

Julie Kunkle, SC Department of Commerce
John LaCour, formerly PhishLabs
Lee McIlwinen, SC Research Authority
John Moore, Momenteum Strategies
Jess O'Brien, Beaufort Digital Corridor
Vayl Oxford, Savannah River National Laboratory
Peter Shand, Business Development Corporation of SC
Eric Skipper, USC Beaufort
Dick Stewart, Stewart Family Office
Sebastian Van Delden, College of Charleston
Dr. Kuang-Ching (KC) Wang, Clemson University

DEFENSE PARTNERSHIPS

Dan Beatty, SC Military Base Task Force
Dr. Shankar Banik, The Citadel
Sean Barnes, Cyber Center of Excellence, Fort Eisenhower
Jim Clifford, City of North Augusta
Erik Gardner, NIWC Atlantic
Gary Jaffe, Charleston Defense Contractors Association
BG David Jenkins, SC National Guard
Kevin Kingery, Aiken Technical College
Lt. Col. Thomas Little, AFCENT/Shaw AFB
MG (ret.) Jennifer Napper, Peraton
Col. (ret.) Warren Parker, South Coast Cyber Center
Col. Chris Smith, AFCENT/Shaw AFB



1201 Wilson Boulevard
27th Floor
Arlington, VA 22209

222 Broadway
19th Floor
New York, NY 10038

simon
everett
an analytic design firm