SOUTH CAROLINA

CYBER ECOSYSTEM STRATEGIC PLAN



simon everett
an analytic design firm

VERSION 2.3, 30 OCT 2026: UPDATES PROVIDED TO SUPPORT DECEMBER 2026 CONFERENCE AT THE CITADEL

Cover art generated by AI (Bing Image Creator)

Table of Contents

Table of Contents

I. INTRODUCTION 1

Background 1
Objectives and Initiatives 2
Complementary State Plans 4

II. EDUCATION & WORKFORCE DEVELOPMENT 6

1. Establish Statewide K-12 Cyber Learning Standards and Supportive Curricula 7
2. Engage Cybersecurity Professionals to Augment K-12 Educator Force 8
3. Develop SC-Specific Cybersecurity Career Pathway Maps 9
4. Facilitate Adoption of Cyber Education Assets at SC Technical Colleges 10

III. POSTURE & READINESS 12

5. Fund and Expand the SC Critical Infrastructure Cybersecurity Program 13
6. Promote Cybersecurity Readiness Across SC's Industry Supply Chain 14
7. Launch a Centralized Website for South Carolina Cybersecurity Resources 15

IV. INDUSTRY GROWTH 17

8. Develop & Market SC's Cyber Ecosystem Brand to Promote Economic Development 18
9. Expand retrainSC Applicability to Incentivize Cybersecurity Upskilling 19
10. Offset Industry Costs for Security Clearance-Related Assets 20
11. Support Tech Transfer Between NIWC Atlantic and South Carolina Industry 21

V. INNOVATION & ENTREPRENEURSHIP 23

12. Create Joint Appointments for SC Cybersecurity Faculty at SRNL 24
13. Catalyze Investment in SC Cybersecurity Startup and Growth Companies 25
14. Develop a Mentor Network for Cybersecurity Entrepreneurs 26

VI. DEFENSE PARTNERSHIPS 28

15. Increase SC Cyber Employer Participation in DoW SkillBridge Program 28
16. Establish Accelerated Training Program to Support DoW Cyber Missions 29
17. Support and Align Defense-Oriented Regional Cyber Ecosystems 31

VII. ACKNOWLEDGMENTS 35

I. Introduction

ABOUT THIS VERSION:

This strategic plan was produced in 2024. Throughout 2026, working groups convened by the SCRA Center for Cybersecurity have reviewed its initiatives to retire those overtaken by events, update others, and move priority work forward. An updated plan will be published in 2027. We are sharing the original version now to facilitate discussions at South Carolina Summit on Cyber, AI, and Intelligence, to be hosted by The Citadel on December 10-11, 2026. Throughout this report, yellow boxes like this one provide status updates as of October 2026. The original descriptions have not yet been changed.

BACKGROUND

South Carolina has spent the better part of a decade building a foundation for cybersecurity[1] leadership. In 2015, the state established the Department of Administration to provide centralized IT and cybersecurity services to state agencies. In 2017, Governor Henry McMaster created the SC Critical Infrastructure Cybersecurity Program—now one of the more developed state-level cyber preparedness operations in the country—to improve threat intelligence and information sharing across the state's critical infrastructure sectors. Over the same period, South Carolina became one of the first states in the nation to establish a Chief Privacy Officer, and the first state to implement cybersecurity requirements for the insurance industry.

More recently, the ecosystem has continued to develop from the bottom up. Eight South Carolina institutions now hold Centers of Academic Excellence in Cybersecurity designations from the NSA and DHS. Workforce development programs like SC Codes and Develop Carolina have expanded the pathways available to South Carolinians pursuing cyber careers. The SC Council on Competitiveness established the SC Tech initiative to strengthen the state's position as a home for the technology—specifically including cybersecurity—industry. And across the research and innovation landscape, SC universities, national laboratories, and federal partners have been building capabilities in cybersecurity for manufacturing, maritime and port security, national defense, and more. The foundation is real, but these bottom-up successes must be met with top-down energy and resources—and intentionality towards a cohesive ecosystem—to convert that foundation into genuine leadership.

In 2021, Governor McMaster's office partnered with SC Commerce and the University of South Carolina to conduct a comprehensive inventory and comparative assessment of the state's cybersecurity ecosystem, examining cyber companies, workforce, economic impact, and the full range of enabling assets. The findings of that study—published in March 2022—confirmed both the depth of what SC had built and the unevenness of how those assets connected to each other and to the stakeholders who needed them. In response, the Governor issued an executive order directing SC Commerce to lead a coordinated effort across industry, academia, nonprofits, and government to enhance the competitive standing of South Carolina's cybersecurity ecosystem. This strategic plan is the result of that effort.

[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 the lead agent for this work reflects a foundational premise: cybersecurity is not a government IT problem. It is an economic competitiveness imperative. South Carolina's leading industry verticals—automotive and electric vehicles, aerospace, advanced manufacturing, supply chain management, and port operations—are increasingly dependent on cybersecurity for their sustained resilience and competitiveness. The state's ability to attract and retain these industries, and to grow the cyber companies that serve them, depends on building an ecosystem that addresses their needs.

OBJECTIVES AND INITIATIVES

This document—South Carolina's first cybersecurity ecosystem strategic plan[2]—presents targeted initiatives for achieving three overarching objectives that together 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.

- **ALIGN** existing cyber-focused assets and initiatives to improve shared situational awareness, utilize resources more efficiently, and promote unity of effort across the ecosystem.
- **AUGMENT** the state's technical cyber capability and capacity through policies and programs designed to support cyber stakeholders at every level—from individual residents to large enterprises.
- **ATTRACT** cyber executives, investors, and workers by strengthening and diversifying the state's portfolio of enabling assets and making South Carolina a compelling destination for cybersecurity talent and industry.

What distinguishes this plan from comparable efforts in other states is its scope. Rather than focusing on a single pillar—workforce, or government IT, or defense partnerships—South Carolina is investing in the full stack of what a cybersecurity ecosystem requires. The five pillars below are mutually dependent: each one is stronger because the others exist, and each one would be weaker in isolation. The overarching goal connecting all five is straightforward: make cybersecurity accessible—to South Carolina's industries, agencies, and citizens.

- **EDUCATION & WORKFORCE DEVELOPMENT**: Building the pipeline of cyber-capable talent that every other pillar depends on—from K-12 curricula and technical college programs to career pathways accessible to students, mid-career professionals, and career changers across South Carolina.
- **POSTURE & READINESS**: Raising South Carolina's collective cyber preparedness across the full spectrum of residents, small businesses, supply chain participants, and critical infrastructure operators

[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 critical infrastructure.

- **INDUSTRY GROWTH:** Creating the conditions for cybersecurity companies to originate, relocate, and grow in South Carolina—and ensuring those companies have the workforce, incentives, and market access to thrive
- **INNOVATION & ENTREPRENEURSHIP:** Building the research, capital, and mentorship infrastructure that converts South Carolina's intellectual assets into cybersecurity companies and products.
- **DEFENSE PARTNERSHIPS:** Deepening the connections between South Carolina's military installations, its cyber workforce, and its civilian industry—in service of both DoW missions and the state's economic development goals.

For ease of reference and planning, each of the 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. Facilitate Adoption of Cyber Education Assets at SC Technical Colleges		
POSTURE & READINESS		
5. Fund and Expand the SC CIC Program		
6. Promote Cybersecurity Readiness Across SC's Industry Supply Chain		
7. Launch a Centralized Website for South Carolina Cybersecurity Resources		
INDUSTRY GROWTH		
8. Develop & Market SC's Cyber Ecosystem Brand to Promote Economic Development		
9. Expand EZone Applicability to Incentivize Cybersecurity Upskilling		
10. Offset Industry Costs for Security Clearance-Related Assets		
11. Support Tech Transfer Between NIWC Atlantic and South Carolina Industry		
INNOVATION & ENTREPRENEURSHIP		
12. Create Joint Appointments for SC Cybersecurity Faculty at SRNL		
13. Catalyze Investment in SC Cybersecurity Startup and Growth Companies		
14. Develop a Mentor Network for Cybersecurity Entrepreneurs		
15. Support SC University-Led, Federally Funded Cyber Innovation Grant Programs		
DEFENSE PARTNERSHIPS		
16. Increase SC Cyber Employer Participation in DoW Skillbridge Program		
17. Establish Accelerated Training Program to Support DoW Cyber Missions		
18. Support and Align Defense-Oriented Regional Cyber Ecosystems Across SC		

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?")

ABOUT THIS VERSION:

Of the list above, this version contains only the objectives and descriptions of each initiative. The key partners, key steps, and metrics have been removed so that current conversations can focus on strategic intent without getting bogged down in (sometimes outdated) implementation details.

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. Facilitate Adoption of Cyber Education Assets at SC Technical Colleges	research 1		skills 1	skills 2
POSTURE & READINESS				
5. Fund and Expand the SC CIC Program	industry 1			
6. Promote Cybersecurity Readiness Across SC's Industry Supply Chain	industry 2	industry 1		
7. Launch a Centralized Website for South Carolina Cybersecurity Resources	industry 1	education 5	awareness 1	awareness 2
INDUSTRY GROWTH				
8. Develop & Market SC's Cyber Ecosystem Brand to Promote Economic Development	industry 1		awareness 1	skills 3
9. Expand EZone Applicability to Incentivize Cybersecurity Upskilling	industry 1		skills 2	awareness 2
10. Offset Industry Costs for Security Clearance-Related Assets	industry 1		skills 3	awareness 2
11. Support Tech Transfer Between NIWC Atlantic and South Carolina Industry	innovation 3	industry 1		
INNOVATION & ENTREPRENEURSHIP				
12. Create Joint Appointments for SC Cybersecurity Faculty at SRNL	research 2	innovation 5		
13. Catalyze Investment in SC Cybersecurity Startup and Growth Companies	innovation 1	innovation 2	skills 3	
14. Develop a Mentor Network for Cybersecurity Entrepreneurs	innovation 3	industry 2	awareness 2	
15. Support SC University-Led, Federally Funded Cyber Innovation Grant Programs	innovation 3	research 3	skills 3	
DEFENSE PARTNERSHIPS				
16. Increase SC Cyber Employer Participation in DoW Skillbridge Program	industry 1		skills 3	awareness 2
17. Establish Accelerated Training Program to Support DoW Cyber Missions	industry 1		skills 1	skills 2
18. Support and Align Defense-Oriented Regional Cyber Ecosystems Across SC	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

- **Building cybersecurity awareness and literacy across South Carolina's full population—from early learners developing foundational digital skills to career-seekers pursuing specialized credentials—while ensuring that SC's employers, agencies, and defense partners have access to a skilled, locally grown cyber workforce**

Every other pillar in this plan depends on this one. The cybersecurity workforce that Industry Growth needs to attract companies, that Posture and Readiness needs to staff SC CIC and advise small businesses, that Innovation and Entrepreneurship needs to fill the companies its capital creates, and that Defense Partnerships needs to support DoW missions at Fort Eisenhower and NIWC Atlantic—all of it starts here, in classrooms, training programs, apprenticeships, and career pathways across South Carolina.

The scale of the need is significant. At current growth rates, South Carolina will need nearly 6,000 additional cybersecurity workers over the next ten years just to meet projected labor demand—before accounting for the additional workforce that this strategic plan's industry growth initiatives are designed to generate. That gap cannot be closed by competing with other states for an existing pool of talent. It must be grown from within.

Growing it from within requires investment across the full education and career spectrum. At the K-12 level, it means establishing cybersecurity as a standard part of every South Carolina student's education—not a specialized elective, but a foundational literacy—and equipping teachers to deliver it. At the technical college and university level, it means closing the documented gaps in cyber education assets: the instructor pipelines, cyber ranges, dual-credit offerings, scholarship programs, and industry-connected capstone experiences that determine whether SC's post-secondary institutions can produce work-ready graduates. And across all levels, it means building the clear, accessible career pathways that allow any South Carolinian—student, mid-career professional, or separating servicemember—to understand how to enter and advance in the cybersecurity field using resources available within the state.

This is not only a workforce strategy. It is a posture strategy. A population with stronger cyber awareness and hygiene is a harder target. A state that produces technically capable, security-minded graduates is better positioned to protect its own digital infrastructure, attract the companies that need that talent, and generate the innovation that drives the next generation of cybersecurity products and services.

South Carolina's goal is not to be a state that talks about cybersecurity education while competing for a finite pool of workers trained elsewhere. It is to build the pipeline—from elementary school to first job—that makes SC a net exporter of cyber talent into its own economy.

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

- ***Align:*** *Promote uniformity, consistency, and equitable access to cybersecurity education across South Carolina, regardless of geography or socioeconomic circumstance.*
- ***Augment:*** *Equip future generations with foundational cyber skills to build both a more cyber-literate citizenry and a stronger pipeline of future cybersecurity professionals.*
- ***Attract:*** *Position South Carolina as an attractive home for cyber industry by demonstrating sustained public investment in developing a skilled, cyber-ready workforce.*

South Carolina has an opportunity to establish cybersecurity as a foundational element of K-12 education—and to do so at minimal cost to the state. Through a partnership with CYBER.ORG, a federally funded organization that provides NICE Framework-aligned cybersecurity curricula and materials at no charge, we can develop and adopt a comprehensive set of learning standards spanning elementary through high school. Once approved by the SC Department of Education (SCDE), these standards and materials can be promoted for adoption across all school districts in the state.

This initiative addresses three distinct but interdependent needs. First, South Carolina's K-12 students lack consistent access to cybersecurity education—creating uneven preparation for higher education, workforce entry, and responsible digital citizenship. Second, many (if not most) K-12 educators are not currently equipped to teach cyber concepts, regardless of whether standards exist. Establishing standards without investing in educator preparation would produce mandates without results. Accordingly, this initiative pairs curriculum adoption with targeted professional development designed to give teachers the confidence and tools to deliver cybersecurity instruction effectively. Third, South Carolina's ambition to be recognized as a leading home for cybersecurity talent and industry requires more than programs and incentives—it requires that the state's own graduates arrive in the workforce with a genuine foundation in cybersecurity. A state that brands itself as cyber-forward while its K-12 students receive little or no cybersecurity education is making a claim it cannot sustain. This initiative is, in part, the proof behind the promise.

The intended result is a generation of graduates who can protect themselves and their organizations online—and a strengthened pipeline of cyber-capable students ready to pursue higher education and career opportunities in cybersecurity. Over time, this pipeline supports both the state's cybersecurity posture and its ability to attract and retain cyber industry.

UPDATE (October 2026):

The working group is engaging several SC school districts to participate in a 2027 pilot program to expand K-12 cybersecurity learning standards and incorporate associated learning activities into existing curricula. Lessons learned and best practices will be captured to inform subsequent program expansion.

2. ENGAGE CYBERSECURITY PROFESSIONALS TO AUGMENT K-12 EDUCATOR FORCE

- ***Align:*** *Leverage existing incentives—certification maintenance requirements, corporare social responsibility commitments, and workforce pipeline interests—to create a strucutred framework that aligns industry participation with school district needs.*
- ***Augment:*** *Supplement SC's K-12 educator force with cyber professionals who can bring technical credibility, real-world context, and career awareness to the classroom.*
- ***Attract:*** *Demonstrate to cyber companies and investors that South Carolina is a state that builds genuine public-private partnerships.*

South Carolina cannot wait for its pipeline of credentialed cyber educators to mature. The good news is that we don't have to—because the private sector already has structural incentives to help.

Cybersecurity professionals holding widely recognized certifications such as ISC²'s Certified Information Systems Security Professional (CISSP) are typically required to complete a defined number of hours in cyber-related education, training, or public engagement each year to maintain their credentials. This creates a ready pool of technically qualified professionals with an existing motivation to engage in exactly the kind of classroom activity SC needs. Meanwhile, cybersecurity companies increasingly seek structured opportunities to contribute to their communities and strengthen the workforce pipeline that feeds their own hiring needs.

This initiative builds a statewide framework that connects both of these resources to SC school districts in a consistent, scalable, and liability-conscious way. Under the framework, cyber professionals and companies can partner with individual schools—whether by "adopting" a school for sustained engagement, contributing rotational lesson modules aligned to SCDE-approved cybersecurity curricula, or delivering virtual sessions across multiple districts. In return, participating professionals can apply their classroom hours toward certification maintenance requirements, and participating companies gain recognized standing as partners in SC's cyber education ecosystem. Districts, in turn, gain access to technical expertise and career mentorship that no curriculum alone can provide.

The framework must be built to last, not improvised. That means standardized partnership agreements, clear vetting and qualification requirements for participating individuals and organizations (with an emphasis on virtual delivery), and centralized coordination resources that allow districts—particularly smaller and more rural ones—to access partners without having to negotiate their own arrangements from scratch.

UPDATE (October 2026):

Furtherance of this initiative is on hold pending implementation of the previous K-12 learning standards item. School districts who participate in that pilot effort will determine whether and how private sector partners are engaged to support these activities.

3. DEVELOP SC-SPECIFIC CYBERSECURITY CAREER PATHWAY MAPS

- ***Align:*** *Make it easy for any South Carolinian to understand how to pursue a cybersecurity career using resources available within the state.*
- ***Augment:*** *Highlight and connect the full range of South Carolina's cyber education and workforce assets through a simple, user-driven framework that converts awareness into action.*
- ***Attract:*** *Signal to cyber talent, executives, and investors that South Carolina has done the work of building an accessible, navigable ecosystem—not just a collection of programs.*

South Carolina has more cybersecurity education and workforce resources than most people realize. The problem isn't supply—it's legibility. Existing national pathway tools are built for curriculum developers, HR professionals, and program managers, not for the high school student trying to figure out a first step, the community college graduate weighing certification options, or the retiring servicemember translating a military cyber career into a civilian one. Those audiences need something different: a road map written for them, mapped to programs they can actually access, and designed to meet them where they are.

This initiative delivers that through three components. First, we will build simplified pathway frameworks—"choose your own adventure" guides that walk users from their current situation to their desired destination using plain language and concrete next steps. These pathways will cover the full range of entry points and career trajectories and will account for both technical skill development and the communication and leadership skills that cybersecurity professionals need to be effective in organizational settings. Second, we will map each pathway to specific South Carolina programs, institutions, employers, and opportunities—ensuring that the pathways are not just legible but actionable, and that users in every region of the state and at every income level can find resources within reach. Third, we will bring this framework to life through a user-friendly online platform—part of the centralized SC cyber portal developed under Initiative 8—where users can explore pathways tailored to their starting point and desired end state, and connect directly with relevant programs, employers, and opportunities across the state.

The result will be a resource that serves students, parents, career changers, and veterans alike—and that gives SC Commerce, SC DEW, and our educational institutions a single, credible destination to point people toward when making the case that South Carolina is the right place to build a cybersecurity career.

UPDATE (October 2026):

The Coordinating Council for Workforce Development, via SC DEW, has issued a procurement notice for design, development, implementation, and operations of the Find Your Future portal, which is envisioned to include the functionality described above. In the meantime, the working group is exploring effective data and visualization frameworks for the cybersecurity-specific pathway maps described above, to support future coordination with the Find Your Future portal.

4. FACILITATE ADOPTION OF CYBER EDUCATION ASSETS AT SC TECHNICAL COLLEGES

- ***Align:*** *Share playbooks, best practices, and lessons learned from leading institutions so that every SC technical college benefits from the progress already made across the system; and align academic outcomes with private sector needs through structured industry partnerships that connect graduating students with SC cyber employers.*
- ***Augment:*** *Close the documented gaps in cyber education assets across the SC Technical College System.*
- ***Attract:*** *Position South Carolina as a state where accessible, hands-on, industry-connected cybersecurity education is available to any resident—making the state increasingly attractive to workforce aspirants, employers, and private sector partners.*

South Carolina's technical colleges are not starting from scratch. Several institutions have earned federally recognized designations for academic excellence, built advanced cyber labs, and developed strong industry partnerships. But the system as a whole is uneven—and that unevenness has real consequences for the residents who rely on their nearest campus.

A survey conducted as part of this planning process—administered in partnership with the SC Commission on Higher Education, with nearly 60% of institutions responding—puts specific numbers on the gaps:

- Instructor hiring is the most pressing challenge, with competitive compensation cited as the primary barrier, followed by difficulty finding candidates with both cyber expertise and teaching experience.
- Only 28% of responding institutions offer cyber-specific scholarships for students.
- Fewer than half offer dual-credit cybersecurity courses that allow high school students to earn college credits before graduating.
- Only 39% of cybersecurity graduates have relevant work experience before completing their degree or certificate.
- Only 30% of responding schools have a cyber range for practical, hands-on training, and only 27% have a Security Operations Center (SOC) or Network Operations Center (NOC) where students can gain real operational experience.
- Capstone programs—in which students undertake cyber-related work for a private-sector partner as a graduation or certificate requirement—exist at only a subset of SC institutions, and vary widely in structure, industry participation, and outcomes.

These are not small gaps. A student at a well-resourced SC technical college has access to hands-on labs, industry internships, work-based learning, and scholarship support. A student at a less-resourced college may have none of those things—even if they're pursuing the same credential. This initiative addresses that disparity through three reinforcing lines of effort.

First, we will build and spread playbooks. We will work with the colleges that have already developed advanced capabilities—cyber ranges, SOCs, dual-credit offerings, capstone frameworks, and industry partnerships—to document what they have built into replicable guides that other institutions can follow. These playbooks will cover both the infrastructure

side (e.g., how to stand up a cyber range, what a SOC requires) and the partnership side (e.g., how to recruit and manage industry partners, how to structure a capstone program that works for both students and employers). The goal is to eliminate the need for every institution to invent these programs independently.

Second, we will close the asset gaps the survey identified. Coordinated resourcing and industry engagement support will help colleges across the system address specific deficiencies—particularly in instructor pipelines, scholarship availability, dual-credit offerings, and hands-on training infrastructure. This includes facilitating relationships between technical colleges and cybersecurity companies that can provide tools, simulation environments, instructors, and internship opportunities; and working with Apprenticeship Carolina and SC DEW to expand the number of cybersecurity companies participating in formal apprenticeship and internship programs with technical college students.

Third, we will establish a statewide capstone project framework. Some SC institutions already require cybersecurity students to complete a capstone project—a substantive, industry-partnered engagement in which students apply their training to real cyber challenges faced by a participating company. These programs benefit students through practical experience and employer connections, and benefit companies through access to emerging talent and a low-cost way to evaluate prospective hires. We will survey existing capstone programs to identify best practices and areas for improvement, develop a standardized framework that any SC institution can implement or improve upon, and establish centralized resources to help colleges recruit and manage industry partners—expanding the roster of participating SC cyber companies and strengthening the connections between today's students and tomorrow's employers.

The goal is a technical college system in which every South Carolinian lives within commuting distance of a cyber-forward campus—one with qualified instructors, hands-on facilities, scholarship support, and direct connections to SC cyber industry.

UPDATE (October 2026):

The working group has yet to discuss this initiative in detail.

III. Posture & Readiness

- **Raising the cybersecurity preparedness of SC residents, small businesses, organizations, and critical infrastructure operators through practical guidance, technical resources, and incident response support**

South Carolina's economy runs on digital infrastructure. The automotive plants of the Upstate, the port operations of the Lowcountry, the financial institutions and healthcare systems serving communities across the state, and the government agencies that deliver essential services to residents—all depend on networks, systems, and data that are under continuous and escalating pressure from cyber threats. Those threats range from financially motivated ransomware attacks and phishing campaigns targeting individuals and small businesses, to sophisticated intrusions by foreign state actors seeking to steal intellectual property, disrupt critical systems, or manipulate information at scale. The question for South Carolina is not whether these threats are real (they are) but whether our residents, organizations, and institutions are adequately prepared to prevent, detect, and recover from them.

The answer, honestly, is uneven. South Carolina has genuine strengths in this area. The SC Critical Infrastructure Cybersecurity Program (SC CIC), housed within SLED, has built one of the more developed state-level cyber preparedness and incident response capabilities in the country—extending its reach to over 430 designated cyber representatives across the state's critical infrastructure sectors and providing threat intelligence, training, tabletop exercises, and incident response support at no cost to participating organizations. That asset is real, proven, and worth building on.

What is less developed—and what this pillar is designed to address—is the broader ecosystem of awareness, guidance, and readiness that surrounds such technical capabilities. Most South Carolina residents and small business owners do not know what resources are available to them, how to access actionable cybersecurity guidance, or who to contact when something goes wrong. Many organizations have invested in technical cyber defenses without investing equally in the executive leadership and governance capacity to make sound decisions when those defenses are tested. And the state's supply chain—the hundreds of smaller firms that support its large manufacturers, port operators, and defense contractors—remains a significant and underaddressed vulnerability.

The initiatives in this pillar address all of these dimensions: expanding and sustaining SC CIC's capacity to serve a broader range of stakeholders; equipping small businesses and supply chain participants with plain-language, actionable cyber guidance; building executive-level cyber governance capability across SC's leading industries; and establishing the centralized web portal that makes all of these resources findable and usable by the audiences who need them. Together, they are designed to raise SC's collective cyber posture across the full spectrum of preparedness—from the individual resident protecting their personal information to the corporate executive making decisions in the first hours of a confirmed incident.

5. FUND AND EXPAND THE SC CRITICAL INFRASTRUCTURE CYBERSECURITY PROGRAM

- ***Align:*** *Ensure South Carolina has a well-resourced, centralized program capable of coordinating cybersecurity guidance and technical assistance to the full range of public and private stakeholders across the state.*
- ***Augment:*** *Enable SC CIC to grow its technical capabilities, expand its regional presence, and serve a broader customer base—commensurate with the expanded role this strategic plan requires of it.*
- ***Attract:*** *Signal to businesses, investors, and residents that South Carolina takes the security of its digital infrastructure seriously enough to fund it—making the state an increasingly credible and attractive operating environment.*

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 assets for cyber preparedness and incident prevention. Focused on providing cybersecurity guidance, resources, and support to critical infrastructure operators across South Carolina—at no cost to those organizations—SC CIC offers robust capabilities across the full spectrum of cyber risk management: threat information sharing, risk assessment, awareness training, tabletop exercises, and incident response.

The numbers speak for themselves. From 2021 to 2024, SC CIC has grown its Cyber Liaison Officer (CLO) network—comprised of designated cyber representatives from the state's critical infrastructure entities—by 250%, now standing at over 430 CLOs who participate in monthly information exchanges, receive threat alerts and advisory communications, and improve their organizations' security posture through facilitated readiness exercises. In 2023 alone, SC CIC responded to 27 critical infrastructure cyber incidents, scanned over 750 malware samples to track threat actor intentions and capabilities, and led the state's successful effort to secure over $3.5 million in federal funding to strengthen the cybersecurity of local government entities across South Carolina.

The problem is not performance—it is resources. SC CIC has demonstrated that it can do this work at a high level. But it is currently funded at a level that requires ongoing federal grant supplementation simply to sustain its existing footprint with minimal staffing. South Carolina is now asking SC CIC to do significantly more: to serve as the coordinating backbone of a statewide cybersecurity ecosystem strategy, extending technical assistance across an expanded and more diverse customer base. That is the right ask—but it requires a commensurate funding commitment.

Dedicated state funding is needed for three specific purposes: to grow SC CIC's technical capabilities so they keep pace with an evolving threat landscape; to establish regional cyber advisors who can build and sustain relationships and coordinate technical support across the state's distinct geographies; and to build the organizational capacity needed to respond promptly to a wider range of public and private stakeholders. The alternative—continuing to ask SC CIC to take on an expanded mission with a grant-dependent, minimum-staffing budget—is a risk the state cannot afford to carry.

UPDATE (October 2026):

Funding request was presented to the Governor's Finance Committee this month. The next legislative review is Feb-Mar 2027 with the House Ways and Means Committee.

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

- ***Align:*** *Ensure that cybersecurity guidance and resources reach South Carolina companies of all sizes—not just those with the resources to fund them independently. .*
- ***Augment:*** *Complement the strong posture of South Carolina's state agencies and large enterprises by meaningfully improving the readiness of the smaller businesses that populate their supply chains—and by strengthening the executive-level governance that determines whether organizations of any size respond effectively when incidents occur.*
- ***Attract:*** *Strengthen South Carolina's commercial competitiveness by reducing the cyber risk carried by our supply chain and by building a business environment in which executives are equipped to govern cybersecurity as a business risk, not merely to delegate it.*

South Carolina's large employers understand their own cyber risk. The more difficult and consequential problem is what happens two or three tiers down their supply chains—where a single compromised vendor can become the entry point for an attack on the organizations above it. This is not a theoretical concern: large South Carolina organizations have experienced cyber incidents that originated downstream, as threat actors exploited vulnerabilities in smaller suppliers' networks to reach their ultimate target.

The common response—requiring vendors to certify compliance with cybersecurity standards—addresses liability, not risk. A vendor that attests to compliance without actually achieving it creates a paper trail for litigation after a breach, not a barrier against the breach itself. South Carolina can do better.

Technology executives at some of the state's largest employers have described a supply chain that sorts into three distinct tiers. At the top are large and some mid-sized companies with the financial and personnel resources to achieve and maintain meaningful cybersecurity compliance. In the middle are most mid-sized and some smaller companies that understand what is expected of them but lack the resources to fully implement every required control—forcing difficult trade-offs and partial solutions. At the bottom are the smallest suppliers, for whom the problem is not resources alone but comprehension: they do not readily understand what is required of them or where to begin. These businesses frequently turn to their large partners for guidance—partners who do not have the capacity to advise hundreds of individual vendors.

When SC's largest employers were asked what the state could do to help, their answer was consistent: provide centralized, plain-language, actionable guidance for small businesses—not another list of frameworks, links, and conceptual references that assumes a level of technical fluency most small business owners do not have. This initiative responds to that ask directly, building on the expertise of SC CIC and the centralized cyber resource portal developed under the next initiative to deliver guidance that a non-technical small business owner can actually use. Concerns about the state's perceived liability for guidance that is followed but proves insufficient are legitimate and will be addressed—but they cannot be allowed to prevent South Carolina from providing its small business community with tools that could meaningfully improve their security posture.

Strengthening the technical readiness of the supply chain is necessary but not sufficient. Cybersecurity incidents ultimately surface in the executive suite—in decisions about disclosure timing, business continuity, legal exposure, ransom authorization, customer communications, and board reporting. These are not technical decisions, and they are rarely made well by executives who have never been forced to confront them before. Accordingly, this initiative also supports the development of executive-tier cyber resilience programming designed to put C-suite leaders and board members through the kinds of decisions they would actually face during and after a confirmed cyber incident—experience that is fundamentally different from the technical tabletop exercises that serve IT and security teams. The goal is not to make executives into technical experts, but to ensure they can govern cybersecurity as a business risk and make sound decisions under pressure when incidents occur. This program complements SC CIC's existing exercise portfolio by reaching an audience that technical exercises typically do not serve and extends its impact into the boardrooms of South Carolina's leading industries.

Together—actionable small-business guidance from below and executive-level governance development from above—these efforts address the supply chain readiness gap at both ends, where it matters most.

UPDATE (October 2026):

In 2027, the SCRA Center for Cybersecurity will coordinate with key partners to develop and host an Executive Cybersecurity Tabletop Exercise Series. This series will consist of events across the state, each one focused on a key industry, aimed at helping corporate leadership teams prepare to make critical decisions and manage the operational and financial impacts of a cyber incident before it happens.

7. LAUNCH A CENTRALIZED WEBSITE FOR SOUTH CAROLINA CYBERSECURITY RESOURCES

- ***Align:*** *Give every South Carolinian—regardless of technical background, geography, or income—a single, accessible destination for the cybersecurity resources, guidance, and opportunities available to them in-state.*
- ***Augment:*** *Multiply the impact of every other initiative in this plan by ensuring that the programs, resources, and opportunities they create are easy to find, easy to understand, and easy to act on.*
- ***Attract:*** *Signal to companies, investors, and talent that South Carolina has not just built cyber assets—it has connected them into a coherent, navigable ecosystem that works for people at every level.*

South Carolina has built more cybersecurity capability than most residents realize. The problem is not supply—it is visibility and accessibility. A student researching cyber education options may not know what a CAE designation means or how to find the SC institutions that hold one. A small business owner who knows they need to comply with industry cybersecurity standards may not know where to begin. An organizational manager who suspects they have experienced a breach may not know what it means, what to do, or who to call. In each case, the resources to help them exist—but finding and using those resources requires a level of technical literacy and institutional knowledge that many South Carolinians do not have and should not need.

Existing national resources make this problem worse, not better. Federal agency websites tend to take an encyclopedic approach—lists of frameworks, links to other sites, and conceptual guidance written for compliance professionals—rather than providing the direct, plain-language, actionable help that a non-expert needs. And even when those resources are useful, they do not tell a South Carolina business owner about the SC CIC program, or a South Carolina student about the technical college in their region with a cyber range and dual-credit offerings.

This initiative builds the portal that changes that—a single, user-centered destination designed for the full range of people who need to engage with South Carolina's cyber ecosystem. Depending on who they are and what they need, users should be able to:

- Report a cyber incident and understand who responds and what to expect;
- Find plain-language guidance on cybersecurity preparedness tailored to their organization type;
- Explore learning pathways and identify educational programs matched to their starting point and goals;
- Locate internships, apprenticeships, and job openings in SC's growing cyber sector;
- Connect with innovation programs and entrepreneurial support resources; and
- Access career transition tools designed specifically for military veterans and separating servicemembers.

The guiding design principle throughout must be simplicity over comprehensiveness. A portal that tries to include everything will replicate the encyclopedic failure of the sites it is meant to replace. Every content decision should be tested against a single question: Can the intended user—a high school student, a small business owner, a recently separated veteran—find what they need and take a next step without assistance? If not, the content is not ready.

This initiative carries particular responsibility within the strategic plan: every other initiative's public-facing impact flows through it. The career pathways developed under Initiative 3, the small business guidance built under Initiative 6, the programs fostered under the Innovation & Entrepreneurship pillar—all of these depend on this portal to reach the audiences they are designed to serve. It must be treated accordingly: as infrastructure, not an afterthought.

A natural and important partner in this effort is the SC Office of Regulatory Staff Broadband Office, whose 2024 Digital Equity Plan sets an explicit goal of ensuring that every South Carolina resident can use broadband services safely and securely. That mandate directly aligns with this portal's purpose, and the Broadband Office's reach into underserved communities strengthens the initiative's ability to serve South Carolinians who most need accessible cyber guidance but are least likely to find it on their own.

UPDATE (October 2026):

The SCRA Center for Cybersecurity will launch this website in 2027.

IV. Industry Growth

- **Building the conditions for cybersecurity companies to start, relocate, and grow in South Carolina—and ensuring SC's industries have access to the cyber expertise and services they need to compete**

Cybersecurity is not a competitor to South Carolina's legacy industries—it is what keeps them competitive. As manufacturing, supply chain management, life sciences, port operations, and agriculture embrace digital connectivity, they also inherit digital vulnerability. The companies and expertise needed to manage that vulnerability are not a separate economic sector sitting alongside SC's industrial base; they are a critical service layer running through it. Growing a robust cybersecurity industry in South Carolina is, in the most direct sense, how we protect the industries we already have.

It is also, in its own right, one of the highest-return economic development investments the state can make. Cybersecurity professionals in South Carolina earn up to 240% of the state's median wage—a wage premium that reflects both the scarcity of qualified talent and the irreplaceable value of what they do. Every cybersecurity company that originates, relocates, or expands here brings not just jobs but the kind of high-skill, high-wage employment that strengthens the state's tax base, supports its communities, and signals to other companies that South Carolina is a serious place to build a technology business.

The initiatives in this pillar pursue that goal through four complementary lines of effort: establishing a brand and narrative that makes SC's cyber ecosystem legible and compelling to companies and talent evaluating where to locate; extending and expanding the workforce incentives that make it easier for SC companies to invest in cyber capability; reducing the barriers to pursuing federal cybersecurity contracts—the single most significant driver of cyber industry concentration in the states that lead nationally; and facilitating the technology transfer connections between SC's defense research assets and the commercial companies positioned to bring those innovations to market. Together, these initiatives are designed to make South Carolina not just a place where cybersecurity companies can survive, but one where they have genuine structural reasons to choose us—and stay.

This pillar does not stand alone. A thriving cybersecurity industry requires the workforce that the Education and Workforce pillar builds, the research and innovation assets that the Innovation and Entrepreneurship pillar develops, the posture and readiness programs that generate informed demand, and the defense partnerships that provide both talent and mission opportunity. Industry Growth is the pillar that converts all of those inputs into economic output—the companies, jobs, and wages that make the full investment in this plan worth making.

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

- ***Align:*** *Ensure that every initiative in this plan is presented as part of a coherent, recognizable whole—giving stakeholders a shared understanding of where South Carolina is headed and why their participation matters.*
- ***Augment:*** *Amplify the impact of SC's cyber investments by communicating them effectively to the audiences—students, workers, companies, investors, and policymakers—whose engagement determines whether those investments succeed.*
- ***Attract:*** *Give South Carolina a distinctive, credible identity in the national cyber landscape that draws talent, companies, and capital by making clear what sets this state apart from every other state making similar claims.*

Every other initiative in this plan will underperform without this one. Programs without narratives don't build ecosystems—they build dispersed, underutilized assets that stakeholders cannot find, evaluate, or rally behind. South Carolina's cyber brand is what transforms a collection of initiatives into a recognizable destination.

The question this initiative must answer is not whether South Carolina should have a cyber brand, but what that brand should say, to whom, and why it should be believed. Many states that have attempted to build cyber ecosystem identities have organized their narrative around a single pillar: education, military presence, or corporate attraction. Others have positioned themselves as leaders in "whole-of-state" cybersecurity—which in practice usually means improving state and local government IT rather than building a genuine private-sector ecosystem. Those approaches produce recognizable but generic claims that several states are making simultaneously and with similar evidence.

South Carolina's differentiating story is still being written—which is exactly why this initiative must begin now, while the ecosystem is actively being shaped and before competing states consolidate their own narratives. What we can say with confidence is that the story will need to be grounded in specifics: the particular industries SC serves, the particular assets SC has built, and the particular combination of attributes—geographic, economic, cultural, and institutional—that no other state can replicate. A brand built on that specificity will be durable. A brand built on generic superlatives will not.

The brand must work at two levels simultaneously. Externally, it must give cyber companies, investors, and talent a compelling reason to choose South Carolina—one grounded in honest evidence and clear about what the state offers today versus what it is building toward. Internally, it must serve as a touchstone for implementation of this plan, ensuring that individual initiatives are presented consistently, that their connections to each other are visible, and that every lead agent is equipped to explain how their piece of the work contributes to the larger outcome. A brand that only faces outward is marketing. A brand that also faces inward is governance.

Developing this brand requires four things: a rigorous assessment of what SC can credibly claim and what distinguishes those claims from what peer states are saying; a clear articulation of SC's cyber identity and value proposition, developed with and tested against the audiences it must persuade; a consistent messaging framework that all partners and growth agents can deploy when speaking to their own audiences; and a deliberate connection to the centralized cyber portal developed under the preceding initiative, which

will be the brand's primary public expression. The brand should also be designed to align with and reinforce SC's broader economic development narratives.

The result of this initiative will not be a tagline. It will be a shared understanding—among state agencies, academic institutions, industry partners, and economic development organizations—of what South Carolina's cyber ecosystem is, what makes it worth investing in, and how to say so consistently and credibly to any audience.

UPDATE (October 2026):

A draft of this statewide cyber ecosystem brand is being developed based on working group discussions and stakeholder inputs and will be revised, finalized, and shared in 2027. A notable feature of the draft brand is SC's intentional focus on developing our cyber ecosystem to most effectively support three key industries in our state: port/maritime operations, manufacturing, and defense.

9. EXPAND RETRAINSC APPLICABILITY TO INCENTIVIZE CYBERSECURITY UPSKILLING

- ***Align:*** *Extend an existing, proven workforce development incentive to serve South Carolina's cybersecurity companies and the growing number of businesses across all industries that need to invest in their internal cyber capabilities.*
- ***Augment:*** *Reduce the cost of cybersecurity upskilling for SC companies—making it more feasible for businesses of all sizes to build and maintain a workforce capable of protecting their networks, systems, and data.*
- ***Attract:*** *Demonstrate to companies considering South Carolina as a home that the state actively supports the kinds of workforce investments that modern, cyber-resilient businesses need to make.*

The SC Technical College System's retrainSC program provides tax incentives—applied against employee withholdings—to South Carolina companies that incur approved costs to upskill employees in connection with new equipment, technologies, or processes. Designed primarily to support "first-line" workers in manufacturing, processing, and technology-intensive industries, retrainSC is a proven tool for workforce development. This initiative pursues two objectives: making the program's existing applicability to cybersecurity companies widely known, and expanding that applicability to serve a much broader share of SC's industry.

What retrainSC already covers—and what many cyber companies may not know. Cybersecurity professionals who work at SC cybersecurity companies and actively deliver services to external customers already qualify for retrainSC incentives—provided they meet standard program conditions (full-time employment, at least two years on payroll, benefits-eligible). Three NAICS codes eligible under the program—541511, 541512, and 518210—directly include cybersecurity products and services, meaning SC cybersecurity companies operating under those codes can already use retrainSC to offset the cost of upskilling their technical workforce. Because the program has historically been marketed to manufacturing and processing industries, many cybersecurity companies may be unaware that it applies to them. Closing that awareness gap is the first objective of this initiative—and it requires nothing more than updated outreach and marketing by SCTCS and partner organizations.

What retrainSC does not yet cover—and should. Current eligibility extends only to first-line employees at companies whose primary business is delivering cybersecurity services. It does not extend to IT and cybersecurity professionals at other kinds of companies—manufacturers, healthcare organizations, financial institutions, ports—who are responsible for securing their employer's own networks and systems. This is precisely the audience most in need of support: the internal cyber workforce of the companies that form South Carolina's broader industrial base. This initiative proposes to expand retrainSC to include cybersecurity employees at any SC company, regardless of industry—limited deliberately to those actively doing the security work, not to executives or IT managers at a remove from it. This expansion directly supports the supply chain readiness goals of the preceding initiative and demonstrates that South Carolina is a state that doesn't just encourage cyber resilience—it helps pay for it.

UPDATE (October 2026):

In 2026 we issued an industry survey to gauge the anticipated use case for the expanded incentive described above. Although response volume was lower than desired, 100% of respondents indicated they "definitely" or "probably" would leverage the program, to collectively upskill between 116 and 272 cybersecurity workers across SC industries. Based on this data, we explore legislative action.

10. OFFSET INDUSTRY COSTS FOR SECURITY CLEARANCE-RELATED ASSETS

- ***Align:*** *Ensure SC's cyber industry has access to the classified facilities, clearances, and infrastructure that federal contracting often requires—putting our companies on equal footing with competitors.*
- ***Augment:*** *Build SC cybersecurity companies' capacity to pursue, win, and deliver on classified federal contracts—growing their capabilities, revenues, and workforce in the process.*
- ***Attract:*** *Signal to cyber companies considering South Carolina that the state actively supports their ability to compete in the federal market, not just the commercial one.*

South Carolina's cybersecurity workforce is less concentrated than that of our regional peers—and the ecosystem study that informed this plan identified a primary reason: neighboring states have a greater density of DoW assets that generate sustained federal contracting demand, which in turn attracts and retains cyber companies and talent. To close that gap, SC companies must be able to compete for federal cybersecurity contracts on equal terms. Right now, many cannot—not because they lack the technical capability, but because they lack access to the specialized infrastructure that federal contracting requires.

The most significant of those infrastructure requirements is the sensitive compartmented information facility (SCIF). A SCIF is a federally accredited secure space required for companies to handle classified information—and in practice, SCIF access is a prerequisite simply to compete for a large share of federal cybersecurity and cyber-adjacent contracts, before a company can even begin performing on them or developing the classified capabilities that generate further contract opportunities. For SC's cyber industry in the Aiken and North Augusta region especially, SCIF access is a competitive necessity: companies there are directly competing with firms just across the Georgia border that

benefit from proximity to Fort Gordon and the classified contracting ecosystem surrounding it. But this disparity is addressable.

Other states that have successfully grown their cyber industries and attracted federal contractor footprints have done so in part through targeted tax credits that reduce the cost of entering and sustaining the classified contracting market. Three types of credits have proven most effective:

- **SCIF construction credits.** Tax credits against the costs of constructing a federally accredited SCIF incentivize medium- and large-sized companies to build this infrastructure within South Carolina rather than outside it—ensuring that the asset, and the contracting activity it enables, remains anchored in the state.
- **SCIF access credits for small businesses**. Small businesses are rarely in a position to construct their own SCIFs. Tax credits against the cost of renting SCIF access—at least in the first year of performing on a classified contract—lower the barrier for smaller SC cyber companies to pursue opportunities they would otherwise have to pass on, while simultaneously creating market incentives for the construction of shared SCIF facilities that benefit the broader innovation ecosystem.
- **Personnel clearance and facility processing credits**. Obtaining and maintaining security clearances, and installing and operating the specialized IT infrastructure required to process clearance requests, carries significant ongoing cost. Tax credits against these costs make it more feasible for SC companies to build and sustain a cleared workforce—the single most important asset in federal cyber contracting.

Deployed together, with reasonable annual and cumulative ceilings per company and for the program overall, these credits would meaningfully close the competitive gap between SC cyber companies and their counterparts in states that have already made this investment. The goal is not merely to offset costs—it is to make South Carolina a genuinely competitive home for companies that want to pursue the full range of federal cybersecurity opportunities, including those tied to DoW missions at Fort Gordon and NIWC Atlantic.

UPDATE (October 2026):

In September 2026, DoW launched the Secure Space Network—an initiative aimed at increasing the availability and accessibility of SCIFs and supportive assets in every U.S. state. Also, in August 2026, Charleston was selected as one of the DoW Defense Innovation Unit's Bridge Program cities (one of ten nationwide). This program's focus areas include developing classified infrastructure-as-a-service assets for local industry.

11. 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 DoW-spurred technological innovations. This collaboration is key in simplifying the complex DoW 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 DoW, 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.

UPDATE (October 2026):

The DoW's Defense Innovation Unit Bridge Program—for which Charleston was selected as one of only ten partner cities nationwide—will be focused on revitalizing industry technical collaboration with the DoW. We will explore opportunities to support those activities to benefit cyber ecosystem growth.

V. Innovation & Entrepreneurship

- **Investing in the research, capital, and mentorship infrastructure that converts South Carolina's intellectual assets and entrepreneurial energy into cybersecurity companies and products**

South Carolina has built genuine strengths in technical innovation—through its national laboratory, its research universities, its manufacturing and defense partnerships, and its history of growing industries that did not originate here into industries that define the state. The Innovation and Entrepreneurship pillar asks a specific question: can those same strengths be focused, resourced, and connected in a way that produces a thriving cybersecurity startup and growth ecosystem—one capable of generating significant companies, retaining talented people, and attracting serious capital?

The honest answer is that the foundation exists but the ecosystem does not yet. South Carolina has SRNL—one of only 17 national laboratories, with a growing cybersecurity research mission—and the universities that partner with it. It has the anchor industries in manufacturing, maritime, and defense that create real and sustained demand for cybersecurity products and services. It has entrepreneurs and investors who have built successful companies here and are willing to help others do the same. What it has lacked is the institutional infrastructure to connect those assets into a pipeline: from research to commercialization, from idea to funded company, from early-stage startup to established firm with the capital and guidance to scale.

The initiatives in this pillar build that pipeline deliberately and in sequence. Joint faculty appointments at SRNL deepen the research collaboration that generates the intellectual property and talent that innovation ecosystems run on. A purpose-built capital architecture provides the funding—structured specifically for the cybersecurity sector rather than adapted from general-purpose economic development models—that converts research outputs and entrepreneurial energy into actual companies. A mentor network ensures that funded companies have the business-building expertise to succeed, not just the resources to try. And a strategic focus on South Carolina's three priority verticals—manufacturing and operational technology security, maritime and port security, and defense cyber—gives every initiative in this pillar a common orientation toward the markets where SC has the most authentic claim to leadership.

12. CREATE JOINT APPOINTMENTS FOR SC CYBERSECURITY FACULTY AT SRNL

- ***Align:*** *Deepen the connection between South Carolina's universities and its resident national laboratory, creating a research and innovation bridge that benefits faculty, students, and the broader cyber ecosystem.*
- ***Augment:*** *Accelerate SC's cybersecurity research and development capacity by placing SC university faculty at the forefront of SRNL's growing national defense cyber mission.*
- ***Attract:*** *Demonstrate South Carolina's seriousness as a cyber innovation hub by making the kind of high-visibility research investment that draws talent, private sector interest, and federal research partnerships.*

Savannah River National Laboratory (SRNL), located in Aiken, is one of only 17 national research and development laboratories under the US Department of Energy. SRNL fosters collaboration with academic institutions through joint appointments—positions in which university faculty split their time between their home institution and the Lab, strengthening research connectivity and creating pathways for students, industry partners, and federal agencies to engage with each other's work. These positions are proven catalysts for innovation ecosystems: they attract private sector investment, generate intellectual property, and produce the kind of long-term institutional relationships that sustain technical progress. Yet only one of SRNL's current joint appointees works in cybersecurity, and that person is not affiliated with a South Carolina academic institution. This is a gap SC is well-positioned to close.

This initiative proposes to establish dedicated cybersecurity joint appointments at SRNL tied to South Carolina universities—beginning with the University of South Carolina, Clemson University, and South Carolina State University—under a title such as "Governor's Cyber Innovation Chair." The appointees would carry active research agendas at the intersection of their university's strengths and SRNL's defense cyber priorities, with explicit expectations for industry collaboration, student engagement, and technology transfer activity.

Funding for these positions may be supported through the 2020 SRS Settlement with the Department of Energy, which dedicated $500 million to South Carolina for economic growth and critical infrastructure development in the Savannah River Site area. Joint cybersecurity appointments at SRNL sit squarely within that mandate. Including industry and nonprofit leaders in the selection process—not just the universities and the Lab—would help ensure that appointees are oriented toward ecosystem impact, not purely academic output.

SC State's participation carries particular significance. SRNL's relationship with historically Black colleges and universities creates an opportunity to expand the pipeline of underrepresented students into cybersecurity research and defense careers—a dimension of this initiative worth building into the appointment framework deliberately rather than as an afterthought.

These joint appointments are designed to serve as connective tissue across the Aiken and North Augusta regional cyber ecosystem—linking SRNL's defense research mission with SC university talent across the state and strengthening the regional innovation assets that support SC's growing role in supporting federal cyber missions.

UPDATE (October 2026):

The SCRA Center for Cybersecurity and SRNL have discussed creating multiple positions for collaborative research between SRNL and several SC universities (though not formally dual-funded "joint appointments"). We will work to bring these to fruition in 2027.

13. CATALYZE INVESTMENT IN SC CYBERSECURITY STARTUP AND GROWTH COMPANIES

- ***Align:*** *Address the structural gap between SC cyber entrepreneurs' capital needs and the investment resources currently available to them.*
- ***Augment:*** *Create the conditions for SC-based cybersecurity companies to form, grow, and stay — building a durable private sector presence that strengthens the state's cyber industry, workforce, and innovation landscape over time.*
- ***Attract:*** *Position South Carolina as a place where cybersecurity entrepreneurs can access the capital, customers, and support they need to build significant companies without having to leave the state to do it.*

South Carolina's cybersecurity entrepreneurs face a capital access problem that generic economic development tools are not designed to solve. Private investors without deep sector expertise struggle to evaluate cybersecurity companies accurately, tend to undervalue them, and impose growth expectations—rapid scaling, early exit—that are poorly suited to how durable cyber companies actually develop. The result is a financing gap that leaves promising SC cyber companies either unfunded or dependent on out-of-state capital that comes with pressure to relocate. Meanwhile, the state has lacked the institutional infrastructure to deploy capital in a way that keeps growing companies—and the jobs they create—anchored in South Carolina.

This initiative builds that infrastructure. Rather than routing state investment through general-purpose funds, it establishes a purpose-built capital architecture organized around three complementary tiers, each designed to serve a different stage of company development within SC's priority cybersecurity verticals: manufacturing and operational technology security, maritime and port security, and defense cyber.

At the earliest stage, seed grants provide new SC cybersecurity services firms with the modest initial capital needed to establish operations, pursue first customers, and connect with the mentorship resources developed under the companion initiative. At the growth stage, a venture studio model actively builds new cybersecurity product companies—not just funding them, but co-creating them with experienced operators who bring both capital and company-building expertise. And for established SC cyber companies ready to scale, a fund built around a Shared Earnings Agreement model provides growth capital in exchange for a share of future earnings rather than equity—preserving founder ownership and control, keeping companies headquartered in South Carolina, and generating returns that recycle back into the program to fund the next generation of companies.

State capital in this architecture is not deployed directly by state employees. It is managed by contracted private investment professionals—selected competitively for their cybersecurity sector expertise—operating within a governance framework that maintains state oversight without substituting state judgment for market judgment. This structural

choice reflects a studied assessment of what has worked and what has failed in comparable state investment programs nationally: programs that preserve professional investment discipline and insulate deployment decisions from political pressure consistently outperform those that do not.

Collectively, this architecture targets the creation of thousands of cybersecurity jobs in South Carolina over a fifteen-year horizon, at a projected net cost per job that compares favorably with the most efficient state economic development programs in the country—and that improves over time as the Shared Earnings repayments reduce the state's net capital at risk.

South Carolina's goal is not to be a state that funds cybersecurity companies. It is to be a state that grows them—and keeps them.

UPDATE (October 2026):

The SCRA Center for Cybersecurity is developing plans for resources to define and expand a business pipeline for SC cybersecurity companies, focused on the verticals of manufacturing, port/maritime operations and associated logistics, and defense, including export markets for the first two of those verticals. Resources will include supportive capabilities for technology pilot projects, opportunity-vendor matchmaking, and entrepreneur support.

14. DEVELOP A MENTOR NETWORK FOR CYBERSECURITY ENTREPRENEURS

- ***Align:*** *Connect SC's resident expertise in cybersecurity business formation and growth—currently dispersed across individuals and organizations—into a structured, accessible resource for entrepreneurs at every stage.*
- ***Augment:*** *Give SC cyber companies the business-building capability they need to make the most of the capital and resources available to them—turning funded companies into successful ones.*
- ***Attract:*** *Make South Carolina a place where cybersecurity entrepreneurs can find not just funding, but the experienced guidance that determines whether funded companies actually succeed.*

Capital is necessary but not sufficient. A cybersecurity entrepreneur who receives an investment without access to experienced business guidance is more likely to make avoidable mistakes—in product positioning, go-to-market strategy, pricing, hiring, and scaling—than one who has both. The mentor network developed under this initiative is the complement to the capital architecture developed under the preceding one: it is what makes the investment work.

South Carolina has the raw material for an exceptional mentorship program. The state is home to experienced cybersecurity executives, successful founders, investors, and business leaders who have built companies in this sector and understand its particular challenges—from the complexity of navigating federal procurement to the difficulty of selling a technical product to a non-technical buyer. What is missing is the structure to connect that expertise to the entrepreneurs who need it, in a form that is accessible, consistent, and scaled to meet demand across the state.

This initiative builds that structure through a tiered program that matches the depth of support to the stage of the business:

- **For early-stage entrepreneurs** just beginning to form a business or enter the market, the program provides group-format education on business fundamentals, peer networking, and connections to the broader ecosystem of resources available through this strategic plan. Much of this tier can be delivered virtually, keeping costs low and access high.
- **For growing companies** with an established offering that need help sharpening their positioning and expanding their market, the program provides facilitated workshops focused on product and service scoping, market development, and go-to-market strategy, delivered by mentors with direct experience in the relevant cyber verticals.
- **For scaling companies** working through the challenges of growth, including team-building, business model refinement, and larger customer and investor relationships, the program provides one-on-one mentoring relationships with experienced leaders who have navigated the same terrain.

Across all three tiers, mentors serve a function that goes beyond individual company support. They are the connective tissue that links entrepreneurs to the capital programs, workforce pipeline, innovation assets, and economic development resources that comprise the rest of this plan, and translate the state's ecosystem-building goals into practical guidance for the companies that will ultimately realize them. A mentor who has built a successful SC cyber company and understands the state's industrial anchors in manufacturing, maritime, and defense is not just a business advisor; they are a guide to what South Carolina's cyber market specifically rewards.

This program requires a permanent institutional home with the public-private relationships and programmatic capacity to recruit and coordinate a sustained mentor community. SCRA and SC Commerce are the strongest candidates, each bringing complementary strengths—SCRA's deep connection to the research and innovation community, and SC Commerce's reach into the corporate and economic development networks that supply both mentors and customers. The decision between them, or a formal partnership between the two, should be resolved early in implementation.

UPDATE (October 2026):

Resources for entrepreneur mentorship and support are envisioned to be included within the capabilities described for the previous initiative.

VI. Defense Partnerships

- **Deepening the connections between SC's military installations, its civilian cyber workforce, and its industry—supporting DoW missions and creating high-growth career opportunities for those who have served**

The Department of War (DoW) is a significant customer of cybersecurity talent and 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 Gordon, 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. South Carolina must develop a sustainable cybersecurity workforce to 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 duty missions, however. We must continue to provide every opportunity for transitioning military personnel to successfully compete for fulfilling jobs following their military service—to include in the high-demand, high-earnings field of cybersecurity.

By improving connectivity between defense, industry, and academic partners we can facilitate career transition, knowledge exchange, and resource sharing.

15. Increase SC Cyber Employer Participation in DoW SkillBridge Program

- ***Align:*** *Strengthen connectivity between the transitioning military personnel 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, attract transitioning service members from across the nation, and facilitate their transition to post-military careers.*

South Carolina is committed to helping military personnel successfully transition to meaningful and rewarding civilian careers following their military service. Such a move is not always easy, as entering the civilian workforce requires navigating entirely new networks, processes, and communications styles. Fortunately, a DoW program designed to assist with this transition is available to employers and separating servicemembers in our state.

The DoW SkillBridge program is a nationwide platform for connecting servicemembers leaving 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 near the end 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 DoW 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 DoW 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

UPDATE (October 2026):

The working group has engaged current and former SkillBridge companies to identify factors for and impediments to success, to inform future assistance. We are currently reaching out to SC cybersecurity companies to assess the industry demand for increased participation in the SkillBridge program. Pending sufficient interest, we will explore the provision of resources to assist companies with registration and management processes.

16. ESTABLISH ACCELERATED TRAINING PROGRAM TO SUPPORT DOW CYBER MISSIONS

- ***Align:*** *Build a capability to efficiently address DoW cyber workforce shortfalls while also further developing South Carolina's cyber education and workforce development landscape.*
- ***Augment:*** *Boost DoW'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 War is challenged to fill every cybersecurity position required to fully prosecute its national security missions. Given our state's proximity to multiple DoW installations with robust cybersecurity activities, South Carolina (and our region at large) is home to a large concentration of military and civilian billets that require a specific

combination of skills and certifications tailored to DoW requirements. The challenge: 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 DoW's Industrial Base Analysis and Sustainment (IBAS) program. ATDM addresses critical workforce shortages in DoW'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 DoW-certified" in four months (eight hours a day, five days a week). And while veterans and even active-duty servicemembers (via the DoW SkillBridge program) can participate, the training is not specifically geared towards them—graduates are intended for the defense industrial base and need not come from the DoW. 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 DoW 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 stand poised to succeed. 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 DoW's ability to secure the cyber talent it needs,

and emplace a key asset for strengthening DoW-industry-academia collaboration in our region.

UPDATE (October 2026):

The working group recently discussed this concept with the DoW's Cyber Academic Engagement Office to validate the need and priority. We will be engaging with ecosystem leaders in the coming months to refine the concept and prepare plans and materials to formally submit for DoW funding consideration.

17. SUPPORT AND ALIGN DEFENSE-ORIENTED REGIONAL CYBER ECOSYSTEMS ACROSS SOUTH CAROLINA

- ***Align:*** *Ensure resources are optimized to maximize South Carolina's ability to support national defense and realize economic gains associated with the cybersecurity missions anchored at and around local major defense installations.*
- ***Augment:*** *Bolster the success of regional initiatives across South Carolina that attract and grow cyber companies, workforce, innovation assets, and investment in proximity to defense cyber missons.*
- ***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 DoW established the Assistant Secretary of War for Cyber Policy (ASW(CP)) for overall supervision of DoW policy for cyber operations. Accordingly, the continued expansion of defense cyber operations has created an increasing array of opportunities for South Carolina to support national defense missions and explore related avenues for economic growth. The state is home to multiple defense-anchored regions, each developing its own cyber ecosystem around a distinct installation, mission set, and set of regional partners. The state's role is to ensure that resources and attention are appropriately positioned to support each of these regional efforts, and to connect them so that they reinforce rather than compete with one another.

A. Aiken/North Augusta/Central Savannah River Area (CSRA)

DoW cyber growth has driven continual expansion of operations and resource needs at Fort Gordon, GA, over the last decade, creating opportunities for the South Carolina side of the Savannah River to support national defense missions and pursue related economic growth. Regional stakeholders have grown key initiatives and assets to maximize these opportunities. The Alliance for Fort Gordon works to ensure the CSRA gains widespread recognition as a competitive district for cyber work, research, and innovation; the Georgia Cyber Center continues to expand as it fosters collaboration among government, academia, and industry; and on the South Carolina side, supporting efforts have been established among partners including the Savannah River National Laboratory (SRNL), the University of South Carolina Aiken (USCA), the South Carolina National Guard, and municipal leaders in Aiken and North Augusta.

The anchor development is now well underway. In May 2025, the South Carolina National Guard and USCA broke ground on a cyber training complex on the USCA campus, adjacent to SRNL's Advanced Manufacturing Collaborative (AMC), with construction expected to complete by the end of 2026. The complex comprises two facilities representing the largest South Carolina National Guard investment in a single location since World War II—a combined investment of $45M:

- The SC National Guard Cyber Integration Center (~$31.8M, ~43,000 sq ft), which will include a SCIF and provide connectivity to Fort Gordon, with classroom space, advanced training areas, and operational and administrative suites serving cyber experts across private, government, and academic sectors.
- The SC National Guard Readiness Center (~$13M, ~24,000 sq ft), which will support training and logistics for South Carolina Army National Guard cyber and signal units and provide USCA students with mentorship and real-world experience alongside Guard personnel.

The complex builds on USCA's standing as an NSA-recognized Center of Academic Excellence in cyber defense and its Regional Security Operations Center (RSOC), which provides cybersecurity protection services to underserved partners such as school districts, nonprofits, and rural infrastructure. The adjacent AMC serves as a public-private innovation hub combining the capabilities of the U.S. Department of Energy's National Laboratories, industry, and educational institutions. With these assets moving from concept to construction, the state's role shifts from helping establish the ecosystem to helping it mature, fill, and connect to the rest of South Carolina's cyber ecosystem.

B. Charleston Region

The Charleston region hosts the state's largest concentration of defense cyber capability, anchored by Naval Information Warfare Center (NIWC) Atlantic at Joint Base Charleston/Naval Support Activity Charleston—one of the Navy's two cyber engineering centers, employing several thousand personnel and supporting a robust defense contractor landscape. Co-located assets include the National Cyber Range Complex (NCRC) Charleston, a cyber range supporting test and evaluation of major DoW acquisition programs as well as training, with particular emphasis on naval and expeditionary platforms. The Palmetto Tech Bridge (PTB), NIWC Atlantic's off-base innovation hub, connects the on-base mission community with industry, startups, and academia, with cybersecurity as a primary focus area.

The surrounding ecosystem is substantial: defense tech makes up a large share of the Charleston area's technology companies, supported by the Charleston Defense Contractors Association (CDCA), and academic anchors include The Citadel and Trident Technical College—both of which are NSA/DHS Centers of Academic Excellence. The Citadel is also home to one of six DoW Cyber Institutes, which are operated at Senior Military Colleges and designed to address national DoW cyber workforce needs.

The state's role in this region is less about building new anchor infrastructure and more about ensuring South Carolina captures the workforce, commercialization, and supply-chain benefits of the existing concentration—including supporting tech transfer between NIWC Atlantic and SC industry; ensuring state programs are positioned to support the

cleared workforce and small-business defense-industrial base; and ensuring connectivity to the rest of South Carolina's cyber ecosystem.

C. Beaufort/Lowcountry Region

Whereas the previous two regional ecosystems are firmly anchored by the local, critical DoW assets they support, the third—in South Carolina's Lowcountry, centered in Beaufort—seeks to build capacity to address an industry gap that offers outsized commercial opportunities for the state. Whereas other states tend to communicate an ecosystem focus on cyber somewhat generically—or, at best, wholly focused on a single industry or sectoral application—South Carolina's differentiator is that it can credibly demonstrate a diversified approach tailored to its industry profile. That profile currently includes manufacturing and defense—but Lowcountry cyber growth initiatives offer the compelling addition of a cyber focus on port/maritime applications.

South Carolina holds a rare convergence in maritime cybersecurity: a top-tier commercial port, a dense defense footprint, demonstrated federal innovation credibility, and a national-security problem set that is both underdeveloped and globally exportable. The Lowcountry has a track record to prove it—USC Beaufort (USCB)) led the South Coast Regional Innovation Engine on a competitively awarded NSF Innovation Engines Development Award, following a $1.3M DoW grant that (among other activities) helped launch the South Coast Cyber Center for regional cyber workforce development. While the region did not advance to a full Phase 2 Engine award, the development-phase win remains a meaningful past-performance qualification: it assembled a statewide, cross-border coalition (USC, Clemson, The Citadel, SC State, TCL, SCRA, SC Competes, the SC Ports Authority, NIWC Atlantic, and SRNL) and stood up the Maritime Cybersecurity Institute, validating that the region's maritime-cyber thesis is nationally credible.

The case is compelling because the commercial and defense rationales point at the same infrastructure. The Port of Charleston—consistently a top-six U.S. port by cargo value with the deepest harbor in the Southeast, anchoring a maritime system that represents roughly 10 percent of the state's economy—is both the economic prize and the real-world test environment. Meanwhile, the Lowcountry's installations (MCAS Beaufort, Parris Island) supply a workforce case distinct from Charleston's NIWC Atlantic mission base, since their servicemembers carry the qualifications the civilian cyber community wants, and a regional pipeline can retain that talent in-state.

The export logic is what turns this from "protect our port" into "build an industry." Port systems are structurally identical worldwide, so solutions validated against the Port of Charleston—alongside two state port authorities, NIWC Atlantic, and federal labs—are inherently exportable to every major container gateway, a market measured in the tens of millions of TEUs at the top U.S. ports alone and reachable through a concentrated base of port operators and their insurers. That demonstration environment is the durable asset—which is why state-level support matters: not to fund the science, but to align Commerce,

the Ports Authority, workforce agencies, and the installations so South Carolina keeps the coalition intact and captures the commercialization and talent benefits in-state.

UPDATE (October 2026):

The working group continues to facilitate information exchange to support this initiative, and we look forward to discussions at The Citadel's upcoming conference that will further inform next steps.

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.

UPDATE (October 2026):

The lists below represent the stakeholders who were involved in the original development of this plan. The next publicly shared version of this plan will include updated working group membership lists to include those who have supported these efforts as of 2026.

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

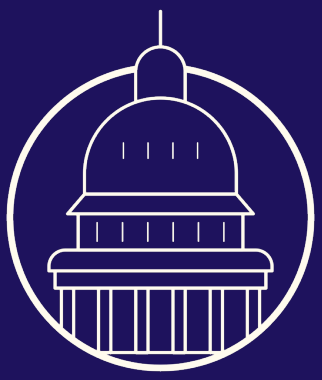
INNOVATION & ENTREPRENEURSHIP

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