

The 3D Cybersecurity Pipeline: Bridging Schools, Higher Education, and Industry

A. Executive Summary

Developing the cybersecurity workforce is a national and statewide priority. There are 3.4 million open cybersecurity positions globally, according to the National Initiative for Cybersecurity Careers and Studies (2024). The International Information System Security Certification Consortium's (ISC2) recent study, *The Cybersecurity Career Pursuers Study* (2021), found professionals in the field noted cybersecurity and information technology (IT) certifications, IT experience, professional networking, and a degree in cybersecurity are most important for gainful employment. The demand for cybersecurity workers in Virginia is higher than the national average. Currently, in the nation there are only enough cybersecurity workers to fill 82% of the jobs and in Virginia, there are only enough cybersecurity workers to fill 75% of the openings. According to CyberSeek, Virginia has the highest total job openings in the United States through the last year, totaling in 50,022. Among those openings, 11,037 are requesting the CompTIA Security+ certification.

The Virginia Space Grant Consortium (VSGC), Virginia Peninsula Community College (VPCC), Brightpoint Community College (BCC), Old Dominion University's (ODU) Commonwealth Cyber Initiative – Coastal Virginia Node (COVA CCI), Great Victory Legends, Coronet Technology Enterprise Inc. (CTEWorkforce-CivilianCyber), Hampton City Schools, and other partners propose a pipeline project to enhance cybersecurity workforce development through secondary education, higher education, and industry connections. The project will increase diversity of participation in the cybersecurity workforce by collaborating with school divisions and community colleges that serve diverse and underserved populations. The three dimensions – *Internships, Education, and Industry* – are components of the cybersecurity infrastructure that support the pipeline from school to career, but these dimensions cannot succeed on their own. This project facilitates active regional partnerships among the three dimensions that integrate National Institute of Standards and Technology (NIST) best practices, partners, and resources to expand participation and meet the growing workforce demands in cybersecurity.

The *First Dimension* will provide undergraduate students with experiential learning opportunities through paid cybersecurity internships with businesses across Virginia. This dimension will leverage Virginia's investment in the VSGC-led Commonwealth STEM Industry Internship Program (CSIIP) to place students in cybersecurity internships. The *Second Dimension* will support the progression of cybersecurity education from the secondary

level into higher education through teacher professional development (PD). The PD will focus on aligning with the NIST National Initiative for Cybersecurity Education Workforce Framework (NICE Framework) and the Virginia Department of Education's (VDOE) cybersecurity competencies. It will include real-world case studies, strategies for student certification exams (CompTIA ITF+, Security+, Network+), and guidance on earning credits for prior learning and through industry certifications for students' further education in cybersecurity. The goal of this constructive collaboration is increasing student achievement in developing cybersecurity skills, obtaining industry certifications, increasing the number of students earning community college credits and majoring in cybersecurity, and preparing them for the workforce. The *Third Dimension* is focused on assessing the workforce skills and competencies specifically for entry-level student internships desired by cybersecurity industry partners in Virginia. This project will survey industry representatives in Virginia to assess current needs and disseminate those findings to stakeholders to better prepare students for success in the cybersecurity workforce.

The VSGC will form two regional alliances composed of academia, government, and industry aligned with the VDOE Superintendent's Regions. Each alliance will include area school divisions, a local community college, and industries providing cybersecurity jobs and internships to bridge the gaps from education to industry (Table 1). The project aims to create a *Virginia Cybersecurity Pipeline: A Regional Blueprint for Education and Workforce Development*, connecting school to career pathways in cybersecurity. This blueprint will be disseminated to stakeholders, outlining Virginia's cybersecurity needs and pathways.

Table 1. Project Structure.

	Region 1 Alliance	Region 2 Alliance	Statewide
Stakeholders	Brightpoint Community College, Greater Richmond School Divisions, CCI Central Virginia Node at Virginia Commonwealth University	VPCC, Hampton Roads School Divisions, COVA CCI	VSGC, VDOE, Virginia companies with cybersecurity internships and jobs
Activities	Teacher PD, Internships, Increasing partnerships with school divisions	Teacher PD, Internships, Increasing partnerships with school divisions	Industry Assessments and Creation of a Regional Blueprint for Education and Workforce Development
Evaluation Criteria Addressed	Project approach builds strong regional, diverse, multistakeholder partnerships; Project PD based on NIST NICE Framework; Project will create positive impact on regional education and workforce; Project will disseminate results through papers and presentations; Project relies on experienced staff; Project budget aligns with scope of work		

The 3D Cybersecurity Pipeline: Bridging Schools, Higher Education, and Industry

B. Project Approach and Execution Plan

VSGC is a coalition of 16 members including five Virginia colleges and universities (Hampton University, Old Dominion University, University of Virginia, Virginia Tech, and William and Mary), two NASA Centers (NASA Langley Research Center and NASA Wallops Flight Facility), VDOE, Virginia Community College System (VCCS) and other organizations representing diverse Science, Technology, Engineering and Mathematics (STEM) interests. The VSGC acts as an umbrella organization, coordinating and developing STEM education, workforce development, and research programs serving the entire state. Part of NASA's national Space Grant program, VSGC's mission is to grow and diversify participation in the STEM workforce. VSGC has a strong track record of connecting precollege education with higher education and industry through regional and statewide projects.

The Commonwealth Cyber Initiative (CCI) is Virginia's main access point for cybersecurity research, innovation, workforce development, and news. The CCI is a network of more than 40 higher education institutions and 375 researchers and is organized into four regional Nodes. ODU leads the CoVA CCI Node serving Region 2, and Virginia Commonwealth University leads the Central Va Node that serves Region 1. ODU also leads the Cyber LeADERS Scholars program funded through the National Science Foundation's CyberCorps Scholarship for Service (SFS) initiative. *STEM in Virginia*: Virginia is expected to add nearly 150,000 new STEM jobs in the next five years, with opportunities expected to grow for years to come, according to the Virginia STEM Education Commission. Employers know they need employees with varying levels of STEM expertise, but the STEM education pipeline has not evolved as quickly as this economic demand. Educational inequities too often limit access to advanced courses in STEM disciplines, credentials, and work-based learning for many vulnerable and underrepresented students.

Virginia is home to the nation's largest naval base as well as several key military organizations and facilities and research facilities including Jefferson Labs and NASA Langley Research Center that are critical to our nation's security and economic well-being. Different regions of Virginia have strengths in various STEM career pathways. For example, the Northern Virginia and Tidewater regions have a strong focus in computer science, cybersecurity, military security, shipbuilding, drafting and engineering. Southwestern and South-Central Virginia are growing in terms of technology use in agriculture, construction, and the energy industry. The manufacturing industry is also growing rapidly, taking a new set of computerized, robotic skills into modern manufacturing settings. Many states

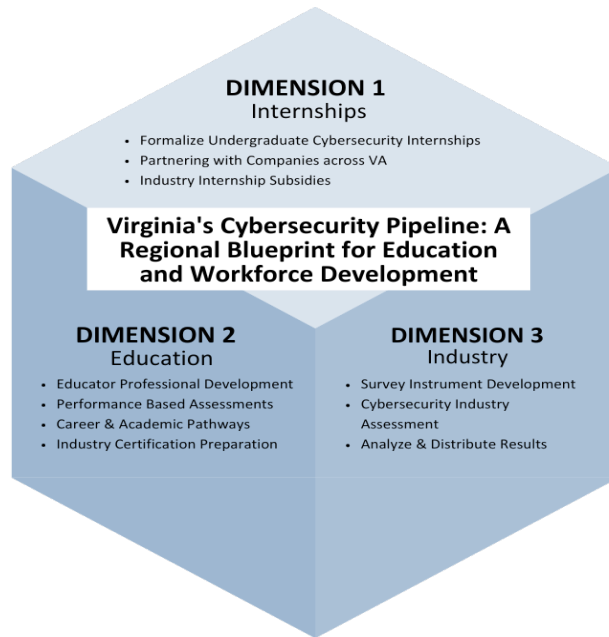
are actively developing STEM plans, goals, and initiatives to advance their STEM agendas. However, with the rapid pace of technological advancements, cybersecurity has become a critical area that demands immediate attention for Virginia to meet the nation's STEM workforce needs.

Cybersecurity and the STEM Workforce: Building a sustainable, diverse, and skilled cybersecurity workforce requires education and training focused on developing transferable knowledge and skills. The NICE Framework outlines and illustrates the importance of acquiring skills through performing the tasks of cybersecurity to be prepared to enter the workforce with necessary knowledge and skills. Further, the NICE strategic plan has identified performance-based assessments as an effective learning method to develop a skilled workforce. In execution of the NICE Strategic Plan, research is being conducted within the cybersecurity community to survey the education and workforce landscape. The NICE Community Coordinating Council recently found that most instructors value hands-on evaluation and that industry partnerships can facilitate performance-based assessments. In support of these goals, VSGC will continue to forge partnerships between industry and educational institutions to improve the quality of cybersecurity education and workforce training.

This 3D project creates a multistakeholder partnership with industry and education, as shown in Figure 1, that will enhance coordination, collaboration, and develop effective strategies for closing the cybersecurity workforce gap and increasing diversity in the workforce.

In alignment with the Department of Commerce's workforce development strategy principles, these partnerships and efforts will build sustainable cyber ecosystems that lead to increased industry-recognized credentials and workplace diversity and development.

Figure 1. Overview of the 3D Virginia Cybersecurity Pipeline.



Dimension 1 Internships: Workforce Development

The *First Dimension* will formalize undergraduate students with experiential learning opportunities through cybersecurity internships at businesses across Virginia. The project will leverage Virginia’s investment in CSIIP and place students in internships working in Virginia’s cybersecurity sector. The NICE goals and objectives will be reached by partnering with the cybersecurity industry to provide students with valuable work-based learning experiences. These internships will help students develop essential skills and prepare them for the rigors of the cybersecurity workforce. Cybersecurity and related majors will be targeted for internship recruitment.

Mentoring and the STEM workforce: Workplace mentors provide support and assistance that help students become oriented to the organization and socialize in the profession, as well as prepare them for career advancement. Mentors can also provide support behaviors that build trust offering acceptance and confirmation, counseling, and serving as a role model (Kram, 1985; Ragins & McFarlin, 1990). A recent National Academies report, *Minority Serving Institutions: America’s Underutilized Resource for Strengthening the STEM Workforce* (NASEM, 2019), reiterated the message that increasing workplace diversity grows the available talent pool and brings a broader range of perspectives and expertise to bear on solving grand challenges in STEM. (Cohen et al., 2002; Florida, 2014). Addressing the underrepresentation of major segments of the nation’s population will require

a multipronged approach, but mentorship will likely constitute a significant component of the complex solutions required. Numerous studies have shown that effective mentorship for underrepresented students enhances recruitment into and retention in STEM related career pathways (Bhatia and Amati, 2010; Dasgupta and Stout, 2014; Dennehy and Dasgupta, 2017). The internships planned by our project will provide an opportunity for students to receive positive mentoring and will allow our project to build our understanding of the components of the mentoring relationship that can positively influence students from underrepresented backgrounds to be recruited and retained in the field cybersecurity.

This dimension proposes *at least 10 subsidies* per year covering up to 50% (up to \$5,000 per student; total of \$50,000 per year) of the cost to companies for internship placements over the two-year performance period. VSGC has found subsidizing part of a company's first CSIIP placement is a valuable incentive for continued involvement, particularly with startups and small companies. It is likely that most subsidy placements will be less than \$5,000 allowing VSGC to place more students. VSGC will provide the subsidies as direct stipends to the companies placing students in paid internships. The remaining 50% balance of the internship stipend will be paid by the company for a one-to-one match. Priority of student internship placements will come from the partnering community colleges in each region, Virginia Peninsula Community College, and Brightpoint Community College. The undergraduate student placements in cybersecurity internships for this project will begin in the fall of 2024 and go through the Summer of 2026. Each placement duration will be an agreement between the student and company.

This alliance includes active partnerships from two industries. CTEWorkforce was founded to provide human-centric, workforce development solutions to meet the growing employer-demand for qualified cybersecurity professionals. CTEWorkforce is headquartered in Richmond, VA, where they provide IT services and IT consulting. CTEWorkforce has been a partner with VSGC placing interns since 2019. Great Victory Legends, Inc. (GVL) is a technology startup incubated at the Virginia Serious Games Institute of George Mason University, which specializes in developing AI-driven virtual reality simulations, software development tools, and QA testing tools. These are just two of the many companies that have placed and mentored CSIIP internships. VSGC's successful working relationships with cyber-related partners and organizations (CCI, Hampton Roads Cyber, Virginia Cyber Alliance) has led to connections with many employers throughout the state of VA. Since 2013, VSGC has placed

over 1,150 students through CSIIIP, with 535 cybersecurity interns placed. VSGC longitudinal tracking reveals that 64% of students still enrolled in school continue interning with the cybersecurity departments following their initial internship and 91% percent of these internship graduates have remained in cyber-related fields. Of the 535 cybersecurity internships placed to date, 33% were underrepresented minorities and 26% were female. VSGC, alongside the regional alliances and multistakeholder partnerships, will continue to work to increase the number of interns from underrepresented and underserved populations as a key measure of success. The two partnering Nodes will assist VSGC in connections to industry for internships.

CSIIIP partnering organizations include but are not limited to: CCI (including all four CCI Nodes), Shenandoah Valley Tech Council, the American Council for Engineering Companies, the Virginia Innovation Partnership Corporation, New College Institute, the Institute for Advanced Learning and Research, the Southern Virginia Higher Education Center, Virginia Chamber, Virginia Aviation Business Association, and the Virginia Association of Colleges, and Employers. VSGC has awarded more than 90 subsidized internships in cybersecurity through three CCI Experiential Learning grants competitively awarded to VSGC. Each placement was matched with industry funding. VSGC has also placed 87 subsidized internships in the aerospace sector with state funding.

Dimension 2 Education: Teacher Professional Development in Cybersecurity

Throughout the state of Virginia, there is a large demand for cybersecurity workers, with industry certifications, such as Security+ and Network+. According to the VDOE, only 563 high school students since 2008 have passed (41.8% pass rate) the Network+ industry certification and 330 high school students since 2013 have passed (57.6% pass rate) the Security+ industry certification upon graduation. This *Second Dimension (2D)* of the project seeks to improve outcomes for students by *strengthening the cybersecurity ramp from high school to higher education and/or the workforce*. This will be accomplished through a collaborative approach of bringing together educators, community colleges, universities, and companies to develop a 2-day teacher professional development (PD) workshop to build teacher capacity in cybersecurity and to identify the number of cybersecurity educational opportunities and pathways in alignment with the NICE strategic goals. Educators recruited for professional development include secondary educators from middle and high schools and community college and dual enrollment instructors in the service regions of our partnering community colleges.

The teacher PD will include immersive learning experiences to build capacity in the following

cybersecurity workforce elements: *content education, performance-based assessments, cybersecurity workplace knowledge and skills* outlined in the NICE Framework, *certifications, and career and educational pathways* extending from secondary school to higher education and/or the workforce. The teacher PD planning, workshop, and classroom implementation support will be spread throughout the project’s performance period (Table 2). The fall of 2024 and winter of 2025 will provide time for collaborators to recruit and survey the teacher participants on their cybersecurity content knowledge and engagement with industry certification testing. The teachers will attend an in-person 2-day workshop held locally in their designated Region. Following the workshop, on-going support will be provided throughout the year of instructional implementation.

Table 2. Teacher Professional Development Milestone Chart.

Fall 2024/Winter 2025	Summer 2025	Fall 2025	Winter 2026	Spring 2026
<ul style="list-style-type: none"> • Collaborative planning with stakeholders for workshop • Working with school divisions on needs • Recruitment of teachers; Teacher pre-survey assessment 	<ul style="list-style-type: none"> • PD workshops: Region 1- June, Region 2- Aug • Teacher post-survey following workshop; Stipend received- \$750.00 per teacher 	<ul style="list-style-type: none"> • Tacher Zoom Check-in • Performance-based lessons due • Feedback given to teachers based on their performance-based lesson 	<ul style="list-style-type: none"> • Teachers implement performance-based assessment approaches • Preparing students for Security+ industry exam 	<ul style="list-style-type: none"> • Maximizing students taking Security+ exam • Teacher reflection and exit survey • Final stipend received- \$750.00 per teacher

The NICE Framework will serve as the foundation for the PD as it outlines and describes cybersecurity work through tasks requiring specific knowledge and skills, which will enable educators and organizations to develop accurate and authentic learning experiences. Each of the educator PDs will follow defined topics but will also be created and planned to best serve their regional needs. The assorted topics to be covered at the teacher PD workshops (Table 3) provide a spectrum of the various areas within the field that are essential to maximize student interest and preparation for the students’ next career and academic steps. Ten teachers per region will be selected and paid a stipend for participation. In addition, regional educators such as school division Career and Technical Education (CTE) and STEM coordinators, administrators, work-based learning specialists and counselors will be invited to attend certain parts of the workshop (Topics 3-5) that showcase certification options and educational and career pathways.

Table 3. Professional Development topics to be covered during the workshop and throughout the school and educator’s participation during this project performance.

Cybersecurity Secondary Education Teacher Professional Development Outline				
<i>Topic 1: Cybersecurity Content Education</i>	<i>Topic 2: NICE Framework for Cybersecurity</i>	<i>Topic 3: Cybersecurity Certifications & Credentials</i>	<i>Topic 4: Educational Pathways</i>	<i>Topic 5: Career Pathways</i>
<ul style="list-style-type: none"> • VDOE aligned curriculum and competencies • Vertical alignment with introductory college curriculum 	<ul style="list-style-type: none"> • Explore the NICE Framework • Embed NICE Framework into curriculum • Develop standards-aligned performance assessments 	<ul style="list-style-type: none"> • Determine certifications for course offerings • Investigate community college credits for prior learning (demonstrated through certifications) 	<ul style="list-style-type: none"> • CyberSeek Interactives • Community college Career Studies certificate, associate degree • Transition to four-year university 	<ul style="list-style-type: none"> • Industry Partners speak to educators • Certifications needed for careers • Advancement opportunities • Internships through VSGC CSIIP

Dr. Michael Mann, Associate Professor of Networking and Cybersecurity at VPCC and recently recognized as an “Expert Level Instructor” by the Cisco Networking Academy, will facilitate the PD in both regions. Dr. Rachel White, Assistant Director of VSGC, will assist in developing and facilitating the workshop, specifically with effective pedagogical approaches to instruction and performance-based assessment. In partnership with Virginia Cyber Range and VSGC, free online (noncredit) video series conducted by Dr. Mann preparing students for two CompTIA certifications, Security+ and Network+, were created through CCI funding in 2022-2024. More than 431 students have registered to view the Security+ preparation videos since July 2023. This dimension will help to close the cybersecurity workforce gap by providing better opportunities for students to pass industry exams and enter the workforce prepared. Industry partners will also participate in the teacher PD workshop to provide firsthand knowledge from the workforce perspective.

This project seeks to increase diversity and inclusion in the cybersecurity workforce. This will be accomplished in part through selection of diverse schools and higher education institutions. In Region 1, Brightpoint Community College (2022 enrollment of 8,792 students) was identified for partnership due to the limited availability and accessibility of cyber education related resources and participation in diverse communities and schools (Table 4). In Region 2, VPCC (2022 enrollment of 6,018 students) was selected for participation due to its diverse community base and existing capacity building efforts in cybersecurity.

Table 4. Demographic information for targeted school divisions in VDOE Superintendent Region’s 1 and 2.

Region 1 School Divisions	Total Population	% Minority Students	% Economically Disadvantaged
Chesterfield	64,183	53.9	32.7
Henrico	50,464	54.5	42.4
Hopewell	3,946	80	85.7
Petersburg	4,464	95.3	83.2

Richmond	21,259	87.5	66.5
Region 2 School Divisions			
Hampton	19,661	67.1	50.4
Newport News	26,219	79	59.6
Williamsburg-James City County	11,694	43.9	35.8
York	13,110	39	30.3

Targeted educators of cybersecurity, programming, computer science principles, Navy Junior Reserve Officers Training Corps (NJROTC), and community college instructors teaching cybersecurity content will be recruited for the PD with a focus on the districts that VPCC and Brightpoint serve and other surrounding districts that fall within VDOE’s Regions 1 and 2. CompTIA Security+ is a global and accredited early career cybersecurity certification with hands-on, performance-based questions included on the exam. Statewide data on student attempt/pass on these industry certifications shows that students are not taking these exams and the ones that do have a very low passing rate. These industry certifications can serve as college credit for specific courses offered at VPCC and Brightpoint Community College.

Dimension 3 Industry: Assessing Cybersecurity Industries across Virginia

VSGC has worked with more than 25 companies offering cybersecurity internships. The companies are of various sizes and represent many different sectors and geographical regions. Some are cyber companies, and others employ a cyber workforce. This network of industry partners represents a great repository of information for educational institutions and other stakeholders to better understand what employers are seeking. This information can significantly impact the teaching and training of the future workforce. Dimension 3 aims to assess participating companies about their experiences with student interns, what workplace training was provided (if any), and desired qualifications and certifications for their entry-level cybersecurity positions. This will be achieved first through the development of an instrument with assessment questions grounded in the NICE Framework Competency Areas specifically including the Task, Knowledge, and Skill (TKS) statements. The NICE Framework Competency Areas are learner focused and delineate necessary proficiencies for students, interns, job seekers, or employees.

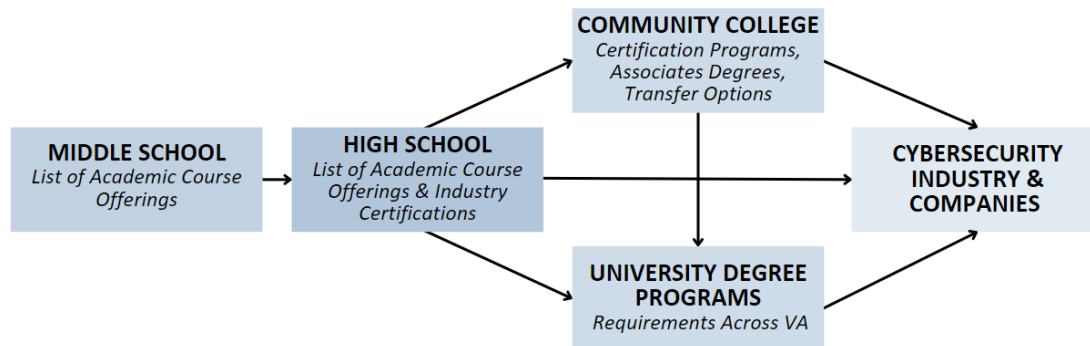
Dr. John Fife, Associate Research Professor at Virginia Commonwealth University (VCU), and Dr. Rachel

White will work collaboratively to develop and test this instrument. Once completed, this survey will be distributed to the companies during winter 2024 and spring 2025. Results will be analyzed and evaluated against the NICE Framework. Companies will be provided with their individual and aggregated statewide data alongside the NICE Framework to expand and encourage the framework's use and provide organizations with the opportunity to assess their own workforce. Time during both teacher regional PDs will be dedicated to reviewing and embedding the findings from the industry assessments within instruction and performance-based assessments. The survey results used in conjunction with CyberSeek interactives, and the NICE Framework will help illustrate a pathway to employment.

Virginia's Cybersecurity Pipeline: A Regional Blueprint for Education and Workforce Development.

Building a cohesive network of cybersecurity stakeholders to strengthen the pipeline of cybersecurity workforce in Regions 1 and 2 is a goal of this project. This will be accomplished by facilitating data-driven conversations among public schools, community colleges, four-year institutions, and industry within each region through our 3-dimensional approach. An outcome of these regional alliances and multistakeholder partnerships will be the development of the *Virginia Cybersecurity Pipeline: A Regional Blueprint for Education and Workforce Development* (Figure 2) to include academic course offerings, programs, certifications, and opportunities with multiple touch and entry points into the cybersecurity workforce pipeline specific to each of the regions participating in this project. An illustration of the various stages in which students could interact with cybersecurity content and be offered information regarding their next steps locally to continue a career in the field. The maps will include specific information within each sector (middle, high school, community college, four-year institution, industry).

Figure 2. The Virginia Cybersecurity Pipeline: Regional Blueprint for Education and Workforce Development.



Evidence of Multistakeholder Partnerships: In 2016, VSGC was a partner in the Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HR Cyber) project. HR Cyber was one of five pilot projects funded by the NIST NICE RAMPS program and was a partnership of educational institutions, government agencies, non-profit organizations, and employers to develop pathways from high school through community college to four-year institutions through educator professional development, internships, and other components. The HR Cyber project and VSGC's role in it are featured as best practices in the NIST publication, *A Roadmap for Successful Regional Alliances and Multistakeholder Partnerships to Build the Cybersecurity Workforce*. The proposed project builds on these successful projects and partnerships.

Through this project, VSGC and partners seek to promote diversity, equity, inclusion, and accessibility through recruitment of public schools and community colleges in areas with a larger population of underrepresented minority communities. In collaboration with VDOE, public schools were identified in regions of the state requiring additional cybersecurity and CTE support. VSGC will continue to work with partners to increase the number of interns from underrepresented and underserved populations as a key measure of success. Through these regional alliances, the project will value the NICE Strategic Plan to "Model Inclusion, advocating and enabling engagement of stakeholders from diverse backgrounds and with varying viewpoints".

C. Project Impacts and Evaluation

The anticipated impacts of the project include (1) increased high quality work-based learning experiences for undergraduate students (2) increased knowledge and skills surrounding the cybersecurity workforce and academic and career pathways for Virginia educators and (3) increased awareness and knowledge of effective cybersecurity education (alignment with state CTE competencies and performance-based assessments), training, and workforce development. To assess and evaluate this project, a mixed methods approach will be applied given the usage of both qualitative and quantitative elements to draw inferences about the study (Creswell & Clark, 2018). This project will be submitted to Old Dominion University Education Human Subjects Review Committee Internal Review Board (IRB) and the participating school division's central office.

Dimension 1. Interns and industry mentors will be contacted during and after internships to ensure progress and determine alignment of tasks to the NICE Framework. Interns will complete a pre/post-internship survey to provide data on whether their skills and knowledge increased and their STEM identity (Estrada et al.,

2011; Chemers et al., 2011). This information will be used for reporting and for continuous improvement of the project. Students will be longitudinally tracked, like all VSGC student participants, to their next step, documenting their flow through the educational pipeline to employment. Metrics of success will include an increase with industry partners, diversifying internships, and placement into the workforce.

Dimension 2. The evaluation and assessment of the teacher PD will be grounded in Desimone (2011) conceptual framework for teacher professional development. The evaluation will follow these three questions to test the teacher participant outcomes: 1) Did the teachers learn? 2) Did they change their pedagogical practices? 3) Did student achievement increase as a result? Desimone discusses the most common tools to measure teacher experiences include surveys, interviews, and observations. The most rigorous methodology is to apply these tools separately to the same study to compare whether they produce similar results. In this project, teacher participants will be evaluated throughout various parts of the performance period. A pre-survey (spring 2025) will be conducted to assess and identify the level at which the teacher participants engage with cybersecurity instruction (secondary education, community college instructor, etc.) and the NICE Framework. Teacher participants will then be administered a post-PD survey (summer 2025) to evaluate the level of content knowledge gained during the 2-day PD session and the identification of implementation support needed.

As a formative checkpoint (November 2025), teachers will submit a performance-based assessment lesson to measure student competencies and capabilities to perform NICE Framework tasks. Dr. Mann and VSGC STEM coordinators will review the submissions and provide the teachers with individual feedback and support. The final points of assessment and evaluation of the teacher PD are exit surveys and focus groups (May/June 2026). The exit survey will assess the effectiveness of the PD, the continued support through classroom implementation, and student attempts towards industry certification. The focus groups will be randomly selected from the participants with one focus group per region. The questions will be semi-structured to allow open discussion of experiences and needs. *Metrics of success* include increased teacher and student self-efficacy in preparedness, completion of certification exams, and familiarity with the NICE Framework Competency Areas.

Dimension 3. Through a collaborative effort with cybersecurity industries across Virginia, Dr. Fife and Dr. White will embed the findings from the industry assessment into *Virginia Cybersecurity Pipeline: A Regional*

Blueprint for Education and Workforce Development. As part of the teacher post-PD and exit-surveys, teacher participants will be asked to what extent this blueprint document was helpful in planning and delivering instruction as well as feedback on how to improve the effectiveness of the document. *Metrics of success* include statewide engagement with the blueprint through conferences, symposiums, career fairs (secondary and higher education), and further discussions with high quality work-based learning specialists across the state.

D. Qualifications

Chris Carter, director of the VSGC, will serve as Principal Investigator (PI) for this project. Carter will provide overall project and fiscal oversight at no cost to the project. Carter has served VSGC in several different capacities for 20+ years and led VSGC's role in the HR Cyber project. *Rachel S. White, Ph.D.*, is assistant director of the VSGC, where she oversees VSGC internship programs including CSIIP. She served as a CTE Governor's STEM Academy coordinator at a Virginia high school and supervised instruction for the CTE and science department. She is a former community college instructor of physics and has 15 years of experience in secondary public education as both a teacher and administrator. She has experience in educational research with a focus on diversifying the field of STEM. On this project, she will serve as the program manager across the regional alliances and lead the assessment and evaluation of the project. *Scott Bellows, Ph.D.*, is VSGC technical programs coordinator where he leads the recruitment of companies and students and coordinates the placement of CSIIP internships. Bellows has more than 12 years of experience with CSIIP including coordinating subsidized placements in cybersecurity and aerospace sectors. His experience has led to numerous connections with business/industry and students that will support the project in addressing the cybersecurity gap in the workforce. He will continue this role at no direct cost to the project. *Michael Mann, D.Sc.*, has over 18 years of experience as an educator in cybersecurity and networking, and brings extensive knowledge and expertise to the project. In his previous career as a SCADA systems software engineer, he honed skills in integrating robust cybersecurity measures into critical infrastructure systems. He has shared his insights on cybersecurity through presentations at esteemed events, including the American Association of University Women conference, and cybersecurity training presentations for the American Association of Port Authorities. Mann has a BS in Computer Science, an MS in Network Management, and a D.Sc. in Cybersecurity, and has demonstrated a lifelong commitment to cybersecurity education. *Kristen Duprey*, VSGC STEM education specialist, is responsible for coordinating K-12 STEM education programs and assisting in CSIIP

internship coordination. She previously served as the STEM curriculum specialist at the Virginia Air and Space Science Center, NASA Langley's visitor center and is a former high school science educator with eight years of experience. She will serve as project coordinator to assist with increasing CSIIIP companies and placements. *John Fife, Ph.D.*, is an associate research professor of STEM education at VCU. He also serves as the director of the Center for Innovation in STEM Education at VCU. Dr. Fife's current research focuses on building resilience and STEM identity in underserved youth by constructing and implementing culturally relevant interventions. He currently serves as the PI on three National Science Foundation (NSF) grants. He will serve as a consultant on this project and liaison to the Richmond area regional alliance of this project's partnership with Brightpoint Community College. He will assist in identifying and recruiting teachers and in the development of the cybersecurity industry survey instrument.

E. Dissemination Plan

Awareness, advocacy, education, collaboration, and recognition are key elements outlined in the NICE Strategic Plan to build a diverse and sustainable cybersecurity workforce. In alignment with those strategies and goals, this project seeks to remove barriers, fulfill educator needs, and promote awareness of local cybersecurity workforce pathways and opportunities in collaboration with stakeholders. The publication of the *Virginia Cybersecurity Pipeline: Regional Blueprint for Education and Workforce Development* document will include the results and findings from this project as it is specific to Regions 1 and 2 and across the state of Virginia. This document will be disseminated throughout the VSGC network, cyber-related partners such as Commonwealth Cyber Initiative and the four CCI Nodes, the Cyber LeADERS Scholars program at ODU, the Virginia Cyber Range at Virginia Tech, Virginia Cyber Alliance, school divisions and higher education.

In addition to the embedded dissemination, results of this project will also be shared publicly on the VSGC website and social media platforms as well as at state and regional conferences, such as the Virginia Cybersecurity Education Conference, Virginia Business Education Association Conference, and through industry networking opportunities (ex: Commonwealth Cyber Initiative Symposium, internship/job fairs). VSGC will present the project at the NASA National Council of Space Grant Directors and will share products and resources through the national NASA Space Grant network. The publication of results in appropriate literature. The project will be presented at the NICE conference in each year of the project.