Fiscal Year 2025 Annual Report to

The Secretary of Commerce and Trade

The Chair of the House Appropriations Committee

The Chair of the Senate Finance and Appropriations Committee

The Director of the Department of Planning and Budget

The Virginia Innovation Partnership Authority (VIPA)

THE COMMONWEALTH CYBER INITIATIVE: FISCAL YEAR 2025 REPORT

Commonwealth Cyber Initiative

October 1, 2025

Message from the Executive Director

The Commonwealth Cyber Initiative (CCI) remains unique in the Nation in bringing together 47 institutions of higher education with a common mission of workforce development, innovation, and research in cybersecurity. In doing so, we continue to be an engine for economic development in Virginia.

The commonwealth is a leader in cybersecurity: the number of cybersecurity professionals per capita here is four times the national average, outpacing states like California and New York. Cybersecurity also represents a critical sector for venture capital investments and federal government expenditures in Virginia.

This year's report details CCI's role in this ecosystem and how we contribute to the commonwealth's economic strength. You will learn that CCI universities' expenditures in research aligned with cybersecurity are now growing at an annual rate of over 8%, compared to the national growth rate of 5.2%. And, according to an economic impact study conducted by RTI International, CCI's programs and activities in the last two years alone supported 2,141 jobs and over $250 million in contributions to the Virginia GDP.

We recognize the foresight of Virginia's leaders in creating our unique initiative six years ago and are extremely proud to be delivering such a robust return on this investment. Cybersecurity will remain a growth area for the foreseeable future, and CCI will continue to be a major contributor to the commonwealth's leadership in this sector.

Luiz DaSilva, Ph.D.; Fellow, IEEE

Executive Director, Commonwealth Cyber Initiative

Bradley Professor of Cybersecurity, Virginia Tech

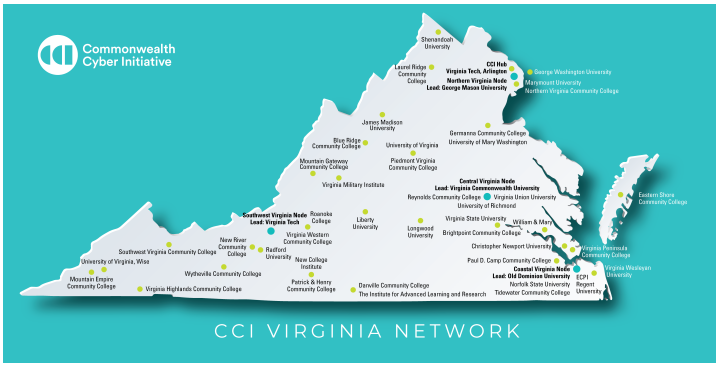
Executive Summary

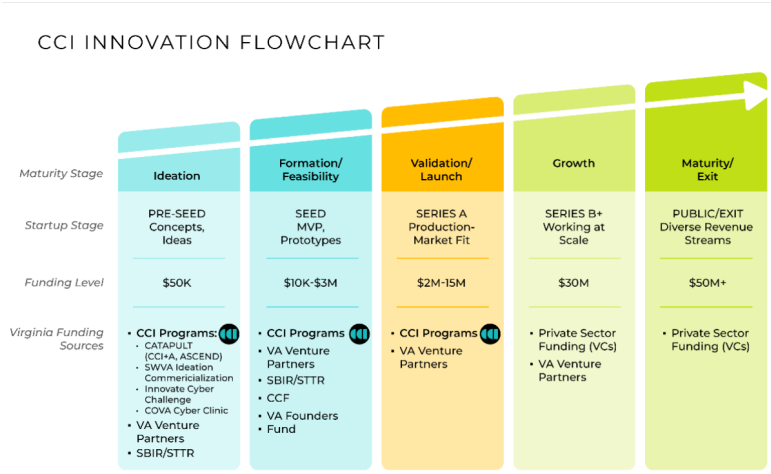
The Commonwealth Cyber Initiative (CCI) was established under the enabling authority of the Appropriation Act - Item 252.B7, Special Session I, 2018. Its objective is "to serve as an engine for research, innovation, and commercialization of cybersecurity technologies, and address the commonwealth's need for growth of advanced and professional degrees within the cyber workforce" (Virginia State Budget, 2018).

Our ambitious vision is to establish Virginia as a global leader in cybersecurity and, by doing so, help diversify the economy of the commonwealth, attracting investment and jobs.

In Fiscal Year 2025 (FY25), we continued to see a significant increase in new research contracts from sources outside the commonwealth, as well as additional emphasis on our workforce development and innovation programs. Virginia is unique in the country in establishing this large-scale collaboration of institutions of higher education (now with 47), and the investment continues to pay off in jobs (and, crucially, a skilled workforce that can fill those jobs!), spinouts and startups, and the reputation of our academic institutions. This report highlights some of the major achievements of the past fiscal year.

Contributing to the Virginia Cyber Economy. The strength and uniqueness of CCI lie in unprecedented cooperation between 47 institutions of higher education in Virginia. Over the past six years, we have become an important contributor to the Virginia cyber economy through our research, innovation, and workforce development programs. In FY25, CCI faculty members attracted more than $84 million in new cybersecurity research grants and contracts to the commonwealth, and CCI activities contributed 960 jobs, corresponding to $79 million in labor income and over $114 million in contributions to the Virginia GDP. Together, CCI universities reported a new high of $108 million in R&D expenditures in computer science in 2023 (the most recent year for which such data are available), a 45% increase since the establishment of CCI. If CCI were a university, it would rank eighth in the country in computer science research expenditures, between Penn State and the University of Illinois Urbana-Champaign. Virginia remains a leader in the cyber workforce, with the largest number of information security analysts in the country, outpacing states like California and New York on both a per capita and total basis. Federal spending on cybersecurity contracts in Virginia exceeded $560 million in 2024, accounting for 29% of the national spending on cybersecurity contracts from the federal government. While we are closely monitoring a potential slowdown in overall research funding by the federal government, we are confident that cybersecurity will remain an investment priority for the Nation's prosperity and national security.





Innovating in Cybersecurity. Innovation is a crucial part of our mission. Our Commonwealth Cyber Incubator + Accelerator (CCI+A) offers two tracks to help faculty researchers move their work from the lab and into the marketplace. CCI's CATAPULT Fund supports teams from Virginia public universities to move new inventions towards commercialization; this year, the fund is supporting five teams working on products such as nano-antennas for tamper-resistant communications and watermarking for large language models. CCI's ASCEND Fund helps startups in Virginia collaborate with faculty experts; this year, we are funding five teams of experts collaborating with startups: OneTier Corp, FraudOptics, Taurus nu-Energy, Critical Shift Corporation, and CodeLock, Inc. Our innovation programs support new inventions through the ideation, feasibility, and validation phases, positioning these teams to attract investment funds from the private and public sectors. In the past two years, CCI researchers filed 26 new intellectual property disclosures. Downstream from this, Virginia continues to significantly outpace our neighboring states in our ability to attract federal Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) funds. In 2024, cybersecurity-related innovation represented 50% of the SBIR/STTR awards to Virginia companies, totaling $133 million.

Strengthening Cyber Startups in Virginia. In addition to the ASCEND Fund, Virginia cybersecurity startups engage with CCI in numerous ways across our three mission lines of workforce development, research, and innovation. We often partner with startups in large-scale research projects funded by federal agencies in the Departments of Defense and Commerce. We also place students in internships in startups and subsidize their stipends. To date, at least 105 startups have directly benefited from CCI programs; some of their logos are shown here. Fend Incorporated, a startup that produced data diodes and unidirectional gateway solutions and that received support from CCI in the early days of our initiative, was acquired by OPSWAT in 2024. Ampsight, a startup previously supported under CCI+A, was acquired by Vibrint for a confidential, undisclosed amount. These are among many success stories that illustrate the growth and strength of the cyber startup ecosystem in the commonwealth.

Launching CCI Spinouts. We have launched 12 spinouts to date: these are new companies in Virginia offering cybersecurity services and/or products, and founded by CCI faculty and students. CCI typically provides support at the early stages of ideation, prototyping, and development of the business model for those companies. In FY25, five new spinouts were launched: WiSights Labs, with founders from UVA and North Carolina State University and a mentor from Virginia Tech, pioneers secure and efficient Artificial Intelligence and Large Language Model solutions for advanced telecommunication networks. CyberMirage, founded by a Mason faculty member, protects the copyright of web images and documents. Wadjet Security, founded by another Mason faculty member, is a cutting-edge cybersecurity company specializing in threat hunting and the protection of cyber-physical systems. RAEMAP LLC, founded by an Old Dominion University (ODU) research scientist, has created a software platform for real-time eye-tracking and cognitive state monitoring. And Chronosys LLC, focused on accelerating wireless scheduling through intelligent software-hardware co-design, was founded by a junior faculty member at Virginia Tech (VT). Three years ago, we provided funding for Symple Solutions, a CCI spinout founded by VCU faculty member Carl Elks; having attracted interest from Dominion Energy and international industry, the company is today on the verge of a major deal.

Investing in AI. Our biggest program in FY25 focused on Artificial Intelligence (AI) for cybersecurity and cybersecurity for AI. These two areas are deeply interconnected: the vast majority of cybersecurity systems today rely on AI for everything from intrusion detection to user authentication; on the other hand, no system that relies on AI can afford to ignore the privacy issues and cyberattack risks involved. This year, we have invested $1.6 million in seed grants in AI. Each of these grants brings together a team from at least two CCI universities to tackle issues such as the use of Large Language Models (LLMs) for intrusion detection that relies on behavioral analysis, AI for biometric authentication, and privacy-preserving federated learning for public health surveillance. AI also figures prominently in virtually all the new inventions that we have funded this year through our various commercialization programs and is an integral part of CCI workforce development programs. In an editorial in the Richmond Times Dispatch, we have made the case that, to win the AI war, we need to prioritize investments in developing a skilled workforce in this area.

Richmond Times-Dispatch
FRIDAY, FEBRUARY 28, 2025 | A5

ARTIFICIAL INTELLIGENCE

To win AI race, invest in talent

The key to winning the artificial intelligence race will not be the data centers or power grids that we can build – it will be the talent that we can develop. In a field that is moving at breakneck speed, it is particularly important to form and recruit the professionals who will drive innovation in building and securing AI systems.

The race for dominance in AI is running full tilt, with a strong focus on infrastructure resources. First came news of Stargate, a $500 billion joint venture by Open AI, Oracle and Softbank, a development momentous enough to merit President Donald Trump's presence at its announcement.

LUIZ DASILVA

trators use it to identify known attacks and combat "zero day" exploits on computer systems.

The flip side is that malicious players also develop attacks that target AI systems. For example, data poisoning attacks manipulate the data used to train an AI system so that it comes up with wrong outputs, or to create a backdoor that can be exploited for unauthorized access to information. AI can also be used to power ransomware attacks and social engineering attacks, through phishing that is increasingly sophisticated and targeted. And jailbreak attacks aim at bypassing security measures built around large language models, or LLMs.

In our network of Virginia universities, researchers are using generative AI to increase the security of iris biometrics, leveraging LLMs to analyze security vulnerabilities in

AI for cybersecurity is already firmly established. AI is routinely used to detect malicious activity: credit card companies use AI to flag unusual purchases, and system adminis-

Luiz DaSilva is the executive director of the Commonwealth Cyber Initiative (CCI) and Bradley Professor of Cybersecurity at Virginia Tech. Contact him at ldasilva@vt.edu.

ANDY WONG, ASSOCIATED PRESS

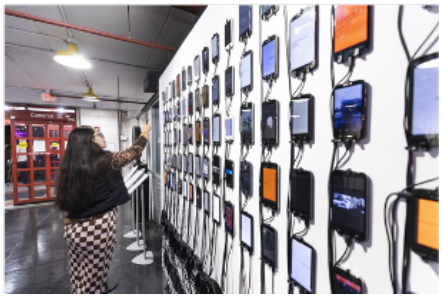
An AI robot moves past an office information board showing the DeepSeek smartphone apps company in Beijing on Jan. 28.

https://cyberinitiative.org/research/funded-projects/ai-for-cybersecurity-and-cybersecurity-for-ai.html

Partnering with Industry. Partnerships with companies of all sizes continue to be a tremendous growth area for CCI. In the last fiscal year, we launched a new Industry-University Cooperative Research Center (IUCRC), co-funded by National Science Foundation (NSF) and industry: the Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks (WISPER) IUCRC focuses on the development of secure 6G technologies. In these highly competitive grants, NSF provides core funding for the administration and management of the center, and industry has the leading role in funding and selecting research projects to be conducted. WISPER currently has 13 industry members and brings in approximately $1 million in funding every year; the center is led by the CCI Executive Director and involves Virginia Tech, Mason, and the University of Arizona. This year, we also joined another IUCRC, Cyber SMART, with a focus on cybersecurity solutions; Dr. Gretchen Matthews, CCI Southwest Virginia Node Director, also serves as site director at Virginia Tech for Cyber SMART. Another large-scale industry collaboration of note is the ACCoRD project, funded by National Telecommunications and Information Administration (NTIA) and led by AT&T and Verizon. Key portions of this $42 million research and testing project are conducted in the CCI xG testbed. In FY25, VCU received the final disbursement of a $17.8 million project funded by the U.S. Department of Defense and supporting a unique industry-academia partnership for industry-specific training and hands-on research for graduate and undergraduate students. This project, the Convergence Lab Initiative, was launched by the CCI Central Virginia Node Director, Erdem Topsakal. Approximately 30% of the research funding that CCI researchers attract comes from the private sector and partnerships, such as the ones described here.

Preparing the Future Cyber Workforce. We continue to expand our experiential learning programs, with 1,114 students engaging in these CCI programs in FY25. We have supported the establishment of a statewide Virginia Cybersecurity Student organization, VCyS, the first of its kind in the commonwealth. VCyS organizes a Capture the Flag (CTF), CyberForge, open to all Virginia students, with support from CCI and private sponsors. In partnership with Virginia Military Institute (VMI), we organize an annual CTF between Virginia universities and community colleges, CyberFusion. Our multiple internship programs, from a pipeline into college to the graduate level, continue to be our most popular student-facing programs. Additionally, CCI's cyber traineeship program enables professionals to make the transition from other jobs into cybersecurity while being placed in their future employers and learning on the job. Through a partnership with the Virginia State Police, we continue to run a year-long internship program that provides undergraduates with hands-on experiences with digital forensics, and in some cases, even in support of real cases being investigated. Through our Cyber Clinics program, 41 students to date have provided cybersecurity services to small businesses in their locality. CCI also funds Radford's Professional Accelerated Cyber Education (PACE) program, offering cybersecurity competency-based training for professionals across Southwest Virginia; in its first year, the program enrolled 62 participants. And this fiscal year, we ran highly popular project-based learning programs with

our partners CACI, Microsoft, PBS, and Guidepoint Security.



Engaging with the Public. Cybersecurity threats can affect us all, and CCI engages with the broader public to inform and demystify issues such as cyberattacks, privacy, data stewardship, the prevalence of artificial intelligence, etc. In our unique CyberArts program, experts in cybersecurity and in the creative arts reimagine and depict the results of cybersecurity research for either scientific or creative arts purposes. The resulting exhibits, displayed in the Torpedo Factory Art Center in Alexandria from October 2024 to January 2025, were seen by 170,000 visitors. A representative comment, left in the visitor book by a Virginia high school teacher: "As a high school teacher, I'm really excited to encourage my students to visit this exhibit. I'm hoping that it will make them excited to potentially study CS [computer science] not just for the 'lucrative' job, but to be a part of something special, creative, and to have the chance to make work that is touching, inspiring, and thought-provoking." We also continue to engage the public through our website, which had 70,000 distinct visitors this year, a nearly 50% increase from the prior year, and through our rapidly growing social media channels.

This report details the many programs, industry engagements, research breakthroughs, student activities, and contributions that CCI has made in the past fiscal year. These programs are conceived and run by the dedicated staff and faculty in the CCI Hub and the Northern, Central, Coastal, and Southwest Virginia Nodes. And above all, the success of CCI is a result of the collaboration between more than 350 faculty members and thousands of students engaged in making Virginia a global leader in cybersecurity.

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project

AI Artificial Intelligence

API Application Programming Interface

CBRS Citizens Broadband Radio Service

CCI Commonwealth Cyber Initiative

CNU Christopher Newport University

CoVA Coastal Virginia

CSIIP Commonwealth STEM Industry Internship Program

CTF Capture the Flag

CTO Chief Technology Officer

CVN Central Virginia Node

FY21 Fiscal Year 2021

FY22 Fiscal Year 2022

FY23 Fiscal Year 2023

FY24 Fiscal Year 2024

FY25 Fiscal Year 2025

FY26 Fiscal Year 2026

Mason George Mason University

HR Human Resources

ICAP Innovation Commercialization Assistance Program

IoT Internet of Things

IUCRC Industry-University Cooperative Research Center

JMU James Madison University

LC Leadership Council

LLM Large Language Model

NoVA Northern Virginia

NSF National Science Foundation

NTIA National Telecommunications and Information Administration

ODU Old Dominion University

O-RAN Open Radio Access Network

PI Principal Investigator

RAN Radio Access Network

SDR Software Defined Radio

SWVA Southwest Virginia

TAB Technical Advisory Board

UVA University of Virginia

VCU Virginia Commonwealth University

VEDP Virginia Economic Development Partnership

VIPA Virginia Innovation Partnership Authority

VIPC Virginia Innovation Partnership Corporation

VMI Virginia Military Institute

VPRI Vice President for Research and Innovation

VSGC Virginia Space Grant Consortium

VSU Virginia State University

VT Virginia Tech

VTRC-A Virginia Tech Research Center - Arlington

WISPER Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks

W&M William & Mary

xG Next Generation Networks

Contents

Chapter 1

The Commonwealth Cyber Initiative

This chapter outlines CCI's vision and mission lines, describes the organization of the network, and outlines the structure for the remainder of the report.

1.1 Vision and Mission

CCI Vision

To establish Virginia as a **global center of excellence** in cybersecurity research and serve as a **catalyst for the commonwealth's economic diversification** and long-term leadership in this sector.

CCI's mission encompasses **research**, **workforce development**, and **innovation** at the intersection between **cybersecurity, autonomy, and intelligence**.

This report describes our progress in each of the mission lines in FY25, in pursuit of the vision of global leadership in cybersecurity for the Commonwealth of Virginia.

1.2 The CCI Network

CCI was established under the enabling authority of the Appropriation Act - Item 252.B7, Special Session I, 2018. Its objective is "to serve as an engine for research, innovation, and commercialization of cybersecurity technologies, and address the commonwealth's need for growth of advanced and professional degrees within the cyber workforce" (Virginia State Budget, 2018).

1.2.1 An Evolving Network

In FY25, CCI grew again, adding Mountain Gateway Community College (MGCC) to our network. The college is supported by the Commonwealth of Virginia, the counties of Alleghany, Bath, Northern Botetourt, and Rockbridge, and the cities of Buena Vista, Covington, and Lexington. The CCI network now comprises 47 institutions of higher education across Virginia, depicted in Figure 1.1.

The leadership structure of CCI comprises a Hub and four regional Nodes. VT serves as the anchoring institution for the Hub and coordinates the strategy and activities of the network; the Hub is hosted in VT's facilities in Arlington. CCI's Central Virginia Node (CVN) is led by Virginia Commonwealth University (VCU), the Coastal Virginia Node (CoVA) is led by ODU, the Northern Virginia (NoVA) Node is led by Mason, and the Southwest Virginia Node (SWVA) Node is led by VT. The CCI Hub is led by an Executive Director, assisted by the Managing Director. Each of the four CCI Nodes is led by a Node Director. Together, they form the CCI Leadership Council (LC), which is responsible for setting the strategy and executing the CCI program. An external Technical Advisory Board (TAB), described further in Section 1.3, advises CCI on strategy and programs. The Virginia Innovation Partnership Authority (VIPA) provides oversight for CCI, as one of the commonwealth's centers of excellence. The governance structure is depicted in Figure 1.2.

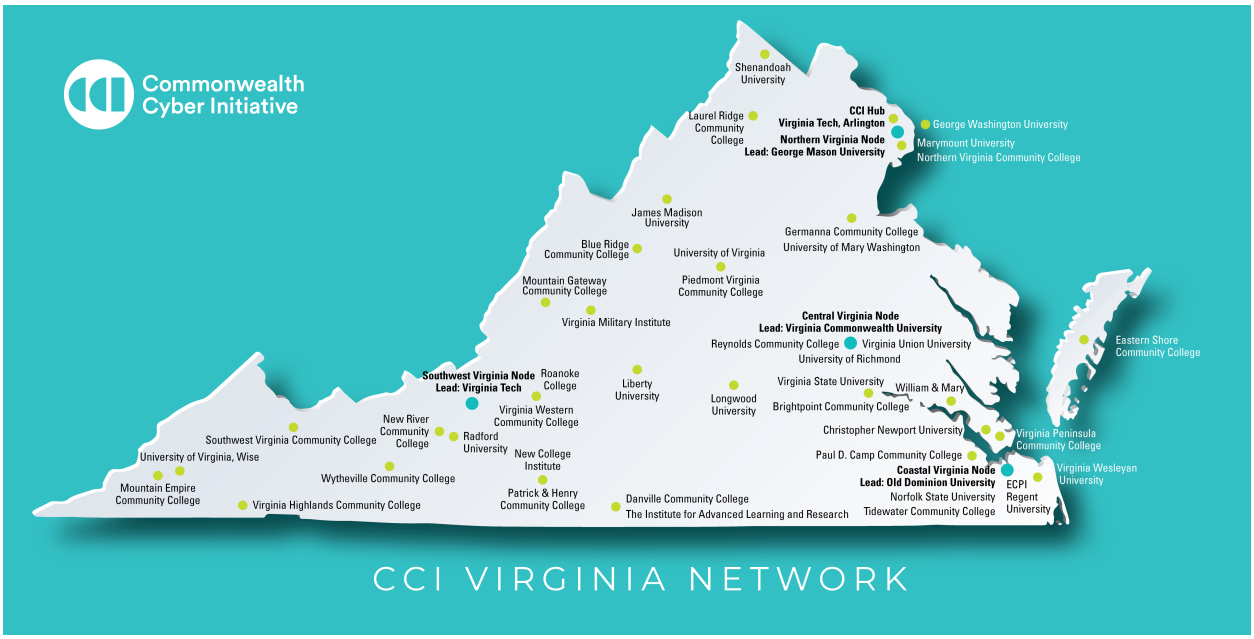


Figure 1.1: The CCI network comprises 47 institutions of higher education across Virginia. Mountain Gateway Community College is the latest member to join.

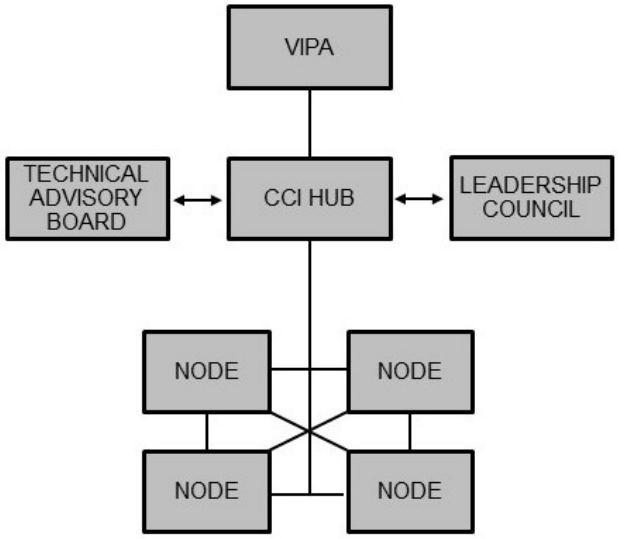


Figure 1.2: CCI governance structure.

The CCI Executive Director chairs the Leadership Council (LC) and is responsible for articulating the research agenda and the innovation and workforce development strategy for the network. The CCI Hub designs, coordinates, and funds network-wide programs and deploys key research infrastructure available to all CCI researchers. The Hub also houses faculty and graduate students with established expertise in key research areas in cybersecurity, autonomous systems, and intelligence. A communications team in the Hub is responsible for external dissemination of CCI activities and successes. Finally, the Hub convenes teams

throughout the network to put together large, multi-million dollar research proposals for external funding. The CCI regional Nodes are responsible for developing capacity in research, innovation, and workforce development in their respective geographic regions, establishing leadership in key focus areas. They also recruit eminent faculty and promising junior faculty for their member institutions and fund programs in the Node, as well as collaborations across multiple Nodes. The main roles of the Hub and the Nodes are summarized in Figure 1.3.

HUB	NODES
○ Chairing the Leadership Council and mapping out the CCI research agenda, innovation and workforce development strategy ○ Developing and coordinating network-wide CCI programs ○ Investing in shared research infrastructure ○ Establishing and supporting expertise in the hub in key research areas ○ Providing funding for some network-wide programs ○ Communicating CCI activities and successes ○ Supporting major, high-risk center-level proposal efforts	○ Developing regional capacity in research, innovation and commercialization, and workforce development ○ Establishing each node's identity and leadership in key focus area(s) ○ Building up research capacity through recruitment of eminent faculty and/or promising junior research faculty ○ Funding programs in the node and collaborations across multiple nodes

Figure 1.3: Roles of the CCI Hub and Nodes.

The CCI Executive Director, Managing Director, and the four Node Directors form the CCI Leadership Council (LC), depicted in Figure 1.4. Dr. Luiz DaSilva serves as the inaugural CCI Executive Director and holds the position of Bradley Professor of Cybersecurity at VT. Mr. John Delaney, former Chief of Staff for the US Army Cyber Command, is CCI's Managing Director. Dr. Liza Wilson Durant serves as NoVA Node Director; she is also a professor and Associate Provost for Strategic Initiatives and Community Engagement at Mason. Dr. Daniel Takabi serves as Coastal Virginia (CoVA) Node Director; he is also the Director of the School of Cybersecurity at ODU. Dr. Erdem Topsakal serves as Central Virginia Node (CVN) Director; he is also a professor and Senior Associate Dean at VCU. Dr. Gretchen Matthews serves as SWVA Node Director; she is also a professor in the Department of Mathematics at VT. The LC meets virtually every other week and in person at least once a year.

1.2.2 CCI Hub Organization and Research Infrastructure Development

The CCI Hub is led by the Executive Director, in close collaboration with the Managing Director. Prof. Jeff Reed, Willis G. Worcester Professor in the Department of Electrical and Computer Engineering at VT, serves as CCI's Chief Technology Officer (CTO), providing advice and leadership of the research focus areas of the initiative. The Managing Director leads the administrative team for the CCI Hub, including an innovation and workforce development director, a communications and marketing director, a program coordinator in charge of pre-award funded research, and a Human Resources (HR) generalist. The director of CCI's xG testbed, as well as Hub research faculty, reports to the executive director. The organizational structure of the CCI Hub is shown in Figure 1.5.

The CCI Hub occupies dedicated space in Virginia Tech's Arlington Research Center for CCI personnel, laboratories, and an Next Generation Networks (xG) testbed, depicted in Figure 1.6. This is the largest testbed of its kind, with the latest generation of software-defined radios and an end-to-end open implementation of 5G, with capabilities to test new technologies expected beyond 5G. It is accessible to CCI researchers and our industry and government partners. The CCI xG Testbed emphasizes programmability and interoperability, relying whenever possible on open interfaces and open-source software. Key areas of capabilities include securing 5G and next-generation mobile networks and AI assurance. In FY25 new test bed equipment was provided in kind to support the ACCoRD project as depicted in Figure 1.8.

(a) Dr. Luiz DaSilva, Executive Director.

(b) Dr. Gretchen Matthews, SWVA Node Director.

(c) Dr. Daniel Takabi, CoVA Node Director.

(d) Dr. Erdem Topsakal, CVN Node Director.

(e) Dr. Liza Wilson Durant, NoVA Node Director.

(f) Mr. John Delaney, Managing Director.

Figure 1.4: CCI Leadership Council.

An outdoor component of the xG testbed is currently being deployed in the Blacksburg campus of VT. This outdoor testbed will offer unique opportunities for testing and validation of new wireless network technologies being developed for 6G and will use VT's Citizens Broadband Radio Service (CBRS) spectrum licenses. Three site locations have been selected around Stroubles Creek in Blacksburg, VA. The second of these three site locations has been set up this year and is located on the Hahn Hall building rooftop. This site has a CBRS base station connected to a 5G core deployed in the edge server and an OpenSAS deployed in the Virginia Tech Research Center - Arlington (VTRC-A) cloud. The setting up and testing of components of the outdoor xG testbed can be seen in Figure 1.7. We plan a formal launch of the outdoor testbed in the Fall of 2025.

1.2.3 CCI Node Organization and Research Infrastructure Development

Each of the CCI Nodes is led by a Node Director, as depicted in Figure 1.4. The regional Nodes have a lean administrative structure, with each Node Director assisted by a program manager. Some Nodes also have a lean communications and marketing team.

The CCI CVN funded the development of a local AI testbed with just over $271,000 to support research in the areas of AI applications in smart health (CVN's Medical Device Security testbed) and smart cities (CVN's OpenCyberCity testbed). This local AI testbed is at VCU and will be available for use in September 2025. CVN also supported Piedmont Virginia Community College with $33,000 in funding to establish a dedicated cybersecurity lab that serves as a hands-on educational environment, enhancing workforce development. Longwood University's infrastructure expanded through the support of CVN with $33,000 in funds to add a Lambda Vector Workstation, which will be used for the training and development of large machine-learning models and data sets.

Also, the NoVA node invested over $77,700 in upgrading the infrastructure of the lab at Mason through adding five 960GB Data Center NVMe Read IntensiveGen4 AG Drives, three PowerEdge R450-Lab, two PowerSwitch S4128, as well as additional hard drives and memory upgrades. These upgrades are in addition to in-kind donations or equipment added to the lab through extramural funding.

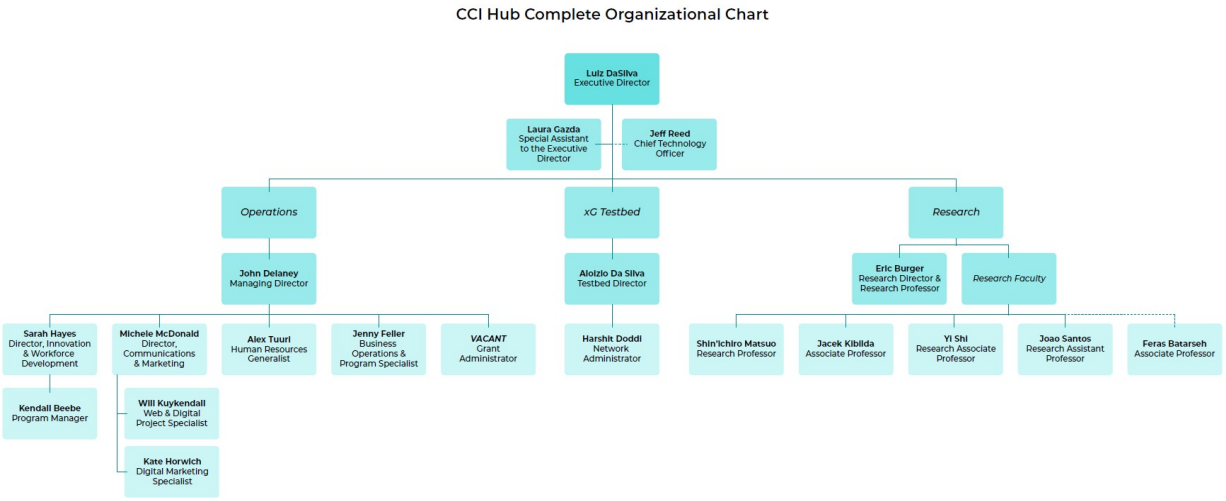


Figure 1.5: CCI organizational chart.

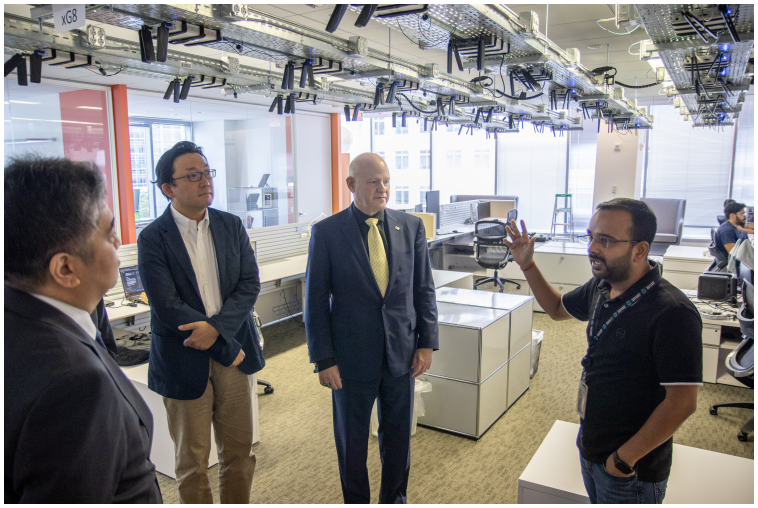


Figure 1.6: CCI xG testbed, indoors portion, in CCI Hub at Virginia Tech.

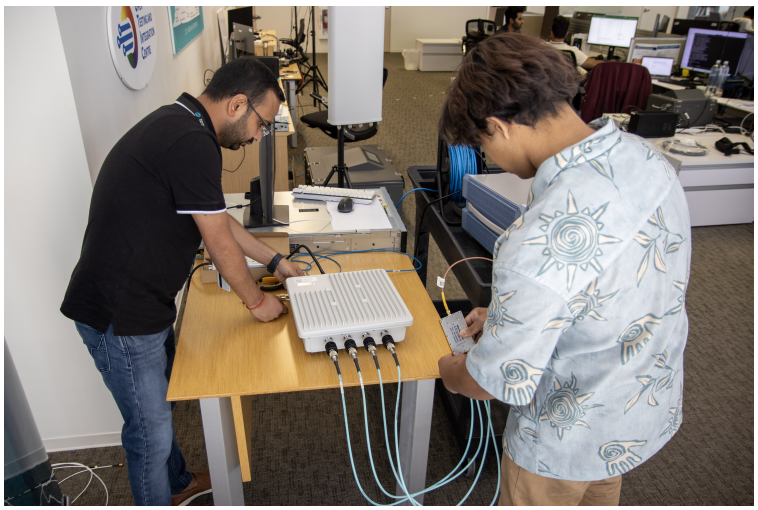


Figure 1.7: Testing components of the xG outdoor testbed in the CCI Hub at Virginia Tech.

Figure 1.8: CCI xG testbed, server room, in the CCI Hub at Virginia Tech.

Figure 1.9: Mason Lab Infrastructure Updates in FY25.

1.3 The CCI Technical Advisory Board

The Technical Advisory Board (TAB) is a key component of our governance structure, shown in Figure 1.2, providing advice and guidance on strategic direction for CCI. CCI's TAB has been in place since Fall of 2020.

The composition of the TAB is as follows:

- One Vice President for Research and Innovation (VPRI) from one of the institutions of higher education in CCI;
- One member appointed by the VIPA board or the Virginia Innovation Partnership Corporation (VIPC);
- Two representatives from industry;
- One representative from the start-up and innovation ecosystem;
- Two leading academic researchers from outside Virginia;
- One representative from the government;
- One at-large member at the discretion of the Executive Director.

We are fortunate to have an extremely distinguished TAB. Its members in FY25 are (Figure 2.12):

- Prof. Elisa Bertino, Samuel D. Conte Professor, Purdue University;
- Mr. David Ihrie, Chief Technology Officer, CIT;
- Prof. Anthony Tongen, Vice President and Chief Research Officer, James Madison University (JMU);
- Prof. Sennur Ulukus, Anthony Ephremides Professor, University of Maryland, College Park;
- Ms. Tracy Gregorio, Chief Executive Officer, G2Ops;
- Mr. Jim Mollenkopf, Vice President, Qualcomm (recently retired);
- Mr. Zachary Tudor, Associate Lab Director, Idaho National Laboratory; and
- Mr. Dan Woolley, Strategic Partnerships Director, The MITRE Corporation (recently retired).

Prof. Elisa Bertino has recently finished her term in the TAB and a new leading academic researcher from outside Virginia will be named in Fiscal Year 2026 (FY26).

The full TAB meets twice a year. FY25's Fall meeting, on September 5, 2024, was held in person at the VT-ARC, in Arlington, Virginia, with TAB members and the CCI Leadership Council in attendance. The agenda included: an update on the State of CCI by the Executive Director, Luiz DaSilva; a presentation on CCI's ACCoRD Project by CCI's Testbed Director, Aloizio Da Silva; student presentations describing their experiences with the CCI Student Project-Based workforce development programs; a presentation by Karen Sanzo, ODU, about the Innovate Cyber program involving forty-three students from seven CCI universities; and a mobile network research presentation by Lingjia Liu, VT. Time was also set aside for open discussion, advice from the TAB, and a celebration of CCI's five-year anniversary.

FY25's Spring meeting, held on March 3, 2025, was held virtually with TAB members and the CCI Leadership Council in attendance. The agenda included: a CCI update by the Executive Director, Luiz DaSilva; an update on the CyberArts and Design Research Program and exhibit at the Torpedo Factory in Alexandria, Virginia by CCI Communications and Marketing Director, Michele McDonald; a review of the upcoming CCI FY24 and FY25 economic impact study by RTI; a research presentation about the CCI funded AI for Cybersecurity and Cybersecurity for AI proposal by CoVA Node Director, Daniel Takabi; a research and innovation presentation by Emanuela Marasco, Mason, focused on CCI's AI for Cybersecurity and Cybersecurity for AI and CATAPULT programs. Time for open discussion and advice from the TAB was also provided.

(a) Prof. Elisa Bertino.

(b) Mr. David Ihrie.

(c) Dr. Anthony Tongen.

(d) Prof. Sennur Ulukus.

(e) Ms. Tracy Gregorio.

(f) Mr. Jim Mollenkopf.

(g) Mr. Zachary Tudor.

(h) Mr. Dan Woolley.

Figure 1.10: CCI Technical Advisory Board (TAB).

The TAB also formed a sub-committee to select the winner of the CCI Impact Award 2025. The award recognizes an individual, team, group, or organization that, through their CCI activities, has conducted breakthrough cybersecurity research or innovation or developed a creative means to improve cybersecurity workforce opportunities for our industry partners and students.

This year's award was presented to CTEWorkforce (Figure 1.12). CTEWorkforce, formerly CivilianCyber, is a veteran-owned company based in Richmond. It has created the Technology Enabled Engagement with Mentoring™ (TEEM) program, which bridges the gap between classroom learning and real-world skills through structured, mentor-led experiences. "We're honored to be recognized by CCI," said CEO Bobby Keener. "This award affirms our impact on students and the cybersecurity workforce."

1.4 CCI Communications

1.4.1 CCI Social Media Strategy, Website, and Metrics

Our communications and marketing strategy has matured, reflecting CCI's impact in its five years of operation. We have strategically expanded the profile of our workforce development, innovation, and research mission lines.

CCI's social media and email campaigns drive people to our website. All areas of our communications outreach show strong growth year-over-year, reflecting a successful strategy.

- LinkedIn grew to 3,775 followers, a 37.7 percent increase.
- Instagram increased to 341 followers, a 20.4 percent increase.
- Website visitors increased to 71,000, a 48.85 percent increase.
- The engagement or user interactions with the website increased to 531,647, a 40 percent increase.

We continue to produce high-quality informational one-pagers, brochures, and graphics. Our monthly newsletter has 4,000 highly engaged subscribers and a strong open rate of about 65 percent during the academic year.

The communications team quickly responds to new program opportunities, such as the Project-Based Learning Program, to help employers connect with talented students. We create graphics and webpages for specific mission lines and programs, building social media and email campaigns to further engagement.

Figure 1.11: FY25 Fall TAB Meeting and CCI 5-year Celebration.

Figure 1.12: Bobby Keener, CEO of CTEWorkforce, with CCI Executive Director Luiz DaSilva.

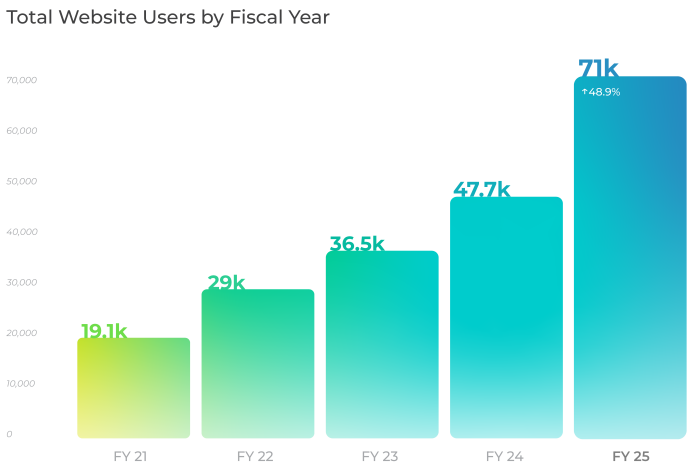


Figure 1.13: Website users by fiscal year.

In addition, our team helps guide opinion pieces from students and CCI leadership for publication in Virginia newspapers, such as the Richmond Times-Dispatch. (Figure 1.13).

Figure 1.14 shows the evolution of our social media followers for our LinkedIn and Instagram accounts.

Expanding the Role of CCI Communications

The communications team also leads three research programs that connect with our workforce development and innovation mission lines: Comprehensive Cybersecurity, which addresses access limitations to cybersecurity technology; CyberArts challenges researchers and artists to reimagine cybersecurity impact; and the Research Paper Showcase, which features the results of CCI-funding through impactful peer-reviewed papers from high-level publications and conferences.

CyberArts Exhibit 2024

Building on the success of the CyberArts 2022 exhibition at the Taubman Museum of Art in Roanoke, Va., the communications team led an ambitious plan for CyberArts Exhibit 2024 held at the Torpedo Factory Art Center on the waterfront in Old Town Alexandria.

The exhibit featured work from Blue Ridge Community College, Mason, JMU, ODU, VCU, and VT.

From Oct. 5, 2024, through Jan. 24, 2025, more than 170,000 people walked through the Torpedo Factory's doors, where the CCI CyberArts exhibits UNDELETED, Steal Your Face, and Unveiling Invisible Sight were strategically placed. Another 7,767 people visited the center's Target Gallery to view three more projects – Hidden Within, Sentiment Voice, and NextGen Security Warnings.

CyberArts 2024 drew comments from national and international attendees, including one from a Virginia high school teacher who wanted her students to visit the exhibit in hopes they will study computer science, not only for a well-paying job, but "to have the chance to make work that is touching, inspiring, and thought-provoking."

Research Paper Showcase 2025

As CCI's influence and programs have grown, so have the results. Virginia researchers are presenting the results of CCI-funded research in high-profile publications and conferences, further increasing CCI's national and global profile.

The third annual CCI Research Paper Showcase features 18 papers, winnowed from more than 30 quality submissions. Selected papers cover such topics as AI for Cybersecurity/Cybersecurity for AI, Cyberattack Resilience, Cybermanufacturing Security, Cryptography, and Wireless Security.

Comprehensive Cybersecurity

The Comprehensive Cybersecurity Program was featured during a workshop at the 2025 CCI Symposium. Virginia researchers are addressing technology challenges that can prevent cybersecurity from reaching as many people as possible, including authentication, vulnerability measures for older adults, and more. As a result of the showcase, the communications team is working with one of the funded researchers to create a

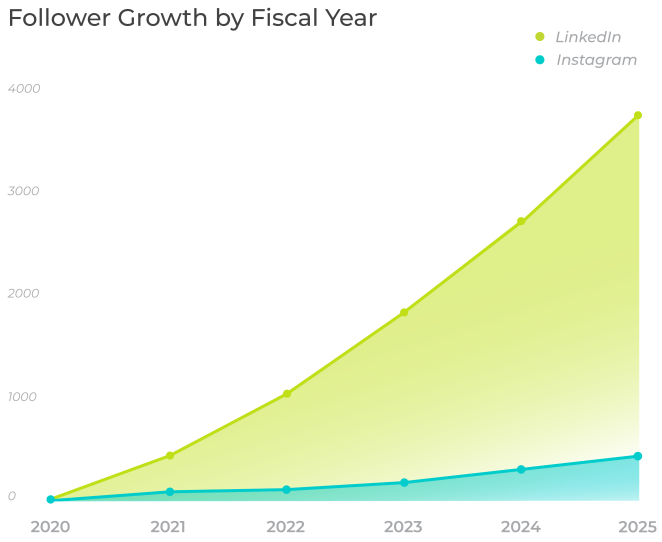


Figure 1.14: Social media followers for CCI's LinkedIn and Instagram accounts.

graphic and cybersecurity awareness campaign based on her research.

1.4.2 Appearances in the Media in FY25

Many of the programs and major achievements from CCI researchers and staff have appeared in the print and online media. Please visit our website's news section for more news.

A sampling of media appearances from the Hub and Nodes is found below:

Commonwealth Cyber Initiative Unites Virginia Universities to Advance AI and Cybersecurity Research (Hub)

Commentary: To Win the AI Race, Invest in Talent Development (Hub)

New Industry-University Collaboration to Pioneer Future Wireless Networks (Hub)

CCI Researchers Join Cyber SMART, A National Industry-University Research Center (Hub)

CCI Funds 10 Cybersecurity Innovation Projects from Four Virginia Universities (Hub and NoVA)

New Art Exhibit Helps Make Cyber Issues Real (Hub)

Cutting-edge CCI xG Testbed Research Opens Door to Next-Generation Mobile Networks (Hub)

How Agriculture and Water Systems Are Fighting AI Pitfalls with AI (Hub)

The Summer Research Experiences for Undergraduates (CVN)

Symple Solutions Turns Simplicity into Security (CVN)

VCU Hosts First CyberRam CTF Challenge Sponsored by Central Virginia Node (CVN)

CCI Researchers Share Findings at CVN Spring Speaker Series (CVN)

Norfolk, Virginia Beach High Schoolers Learn About Cybersecurity at ODU (CoVA)

Cyber Clinic Supports Experiential Learning and Hampton Roads Businesses (CoVA)

Christopher Newport University: Introducing the School of Engineering and Computing (CoVA)

Renowned computer scientist, alumnus to lead W&M's new School of Computing, Data Sciences & Physics (CoVA)

Nearly 500 High Schoolers Get Expert Advice at Virginia Cyberslam 2025 (NoVA)

Keeping Data Safe by Keeping It Separate (NoVA)

Professor Explores the Cybersecurity Potential – And Risks – of Generative AI (NoVA)

Keeping Your Data Safe at The Airport (SWVA)

AI Failed to Detect Critical Health Conditions: Study (SWVA)

Virginia Tech Mathematicians Target Data Center Inefficiency (SWVA)

Reporting requirement	Section(s)
External grants attracted to support the work of CCI	2.1
Research grants awarded from the funds contained in HB30	2.2
Research faculty recruited	2.3
Results of entrepreneurship and workforce programming	3, 4
Collaborative partnerships and projects	5.1
Correlated economic outcomes	5.2
Geographic distribution of the awards from the funds contained in HB30	6.3

Table 1.1: Mapping of reporting requirements to sections of this report.

Securing Internet Routing Becomes Federal Priority: Expert Provides Real-Time Tools for Industry and Government(SWVA)

1.5 Report Structure

This report describes the CCI's progress and achievements in FY25. Chapter 1 outlines our vision and mission, describes the organization of the CCI Hub and Nodes, and summarizes our media strategy. Progress on the three mission lines of research, workforce development, and innovation is described in Chapters 2, 3, and 4, respectively. Chapter 5.1 is devoted to CCI's collaborative partnerships and projects. Chapter 6 contains the financial reports from the Hub and nodes for FY25. Finally, Chapter 7 describes our main activities and programs planned for FY26.

The seven reporting requirements specified in Item 135, Chapter 1289, HB30, are:

- External grants attracted to support the work of CCI;
- Research grants awarded from the funds contained in HB30;
- Research faculty recruited;
- Results of entrepreneurship and workforce programming;
- Collaborative partnerships and projects;
- Correlated economic outcomes; and
- Geographic distribution of the awards from the funds contained in HB30.

The mapping of these reporting requirements to sections of this report is shown in Table 1.1.

Chapter 2

CCI Research

This chapter summarizes the main achievements in FY25 for the CCI research mission line.

2.1 External Grants to Support the Work of CCI

CCI's vision is one of Virginia as a global center of excellence in research at the intersection of cybersecurity, autonomous systems, and intelligence. The economic impact that CCI can bring is predicated on being recognized by industry, government agencies, and the broader research community as being leaders in this research domain. To achieve this mission, CCI is investing in unique research infrastructure and in research programs that build capacity and seed new areas of excellence. This has already resulted in unprecedented success in obtaining extramural funding to support CCI research. This section summarizes the outcomes of CCI's research mission.

2.1.1 Extramural Funding in FY25

In FY25, the CCI network received 159 external grants totaling $84,497,925 to support the CCI mission lines of research, workforce development and innovation. 128 grants (80%) were from federal agencies and 31 (20%) were from state and industry partners. Summary information is shown in Figure 2.1, and details are found in Appendix 1.

Node	Number of Grants	Grant Total
CCI Hub	15	$3,159,900
Central Virginia	9	$9,446,162
Coastal Virginia	21	$11,786,185
Northern Virginia	68	$36,675,861
Southwest Virginia	46	$23,429,817
Total	**159**	**$84,497,925**

Figure 2.1: External funding obtained by the CCI network in FY25.

Note: Researchers often obtain additional extramural funding beyond the grants reported above. For example, in FY25 CCI SWVA researchers attracted $109,105,953 in external research funding, including (but not limited to) those funds directly linked to prior CCI projects as reported in Appendix 1: CCI Extramural Funding for FY25, Southwest Virginia Node table. The values in Figure 2.1 reflect only extramural funding that is attributed to investments made by CCI.

2.2 Research Grants Awarded from the Funds in HB30

In FY25, CCI awarded grants to the participating institutions, aligned with our goals in research, workforce development, and innovation. These funds were awarded on a competitive basis, with researchers responding to calls for proposals issued by CCI. Proposals were reviewed by experts in the area of each call, and the LC made final funding decisions based on recommendations from reviewers. This section describes the grants awarded in this Fiscal Year from CCI funds.

2.2.1 Research in AI for Cybersecurity and Cybersecurity for AI

Objective of the Call

The focus of this call for proposals is capacity building in supply chain cybersecurity. Topics include but are not limited to:

- Zero-trust architectures;
- Securing softwarized and disaggregated networks;
- Testing and validation of system security;
- Cybersecurity risks to the semiconductor supply chain, including hardware Trojans;
- Autonomous vehicle supply chain security;
- Supply chain security over the product lifetime, e.g., software updates;
- Supply chain security for systems involving artificial intelligence/machine learning.

Objectives of this call include:

- To produce seminal contributions to supply chain cybersecurity, targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources.
- To produce research contributions that benefit Virginia companies.
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) in supply chain cybersecurity.

This call utilizes CCI Hub funds and is open to Principal Investigators (PIs) in any of the public institutions that are part of CCI.

Selection Criteria

Each proposal was reviewed by at least three subject matter experts and evaluated according to the following criteria:

- Strong intellectual merit related to cybersecurity.
- Relevance to the focus of the call on supply chain cybersecurity.
- Clear plan for obtaining additional funding from government, private sector, philanthropy, etc., and likelihood of being competitive for the programs identified by the PI.
- Strong broader impacts related to CCI's mission lines of innovation and workforce development, as well as in diversifying the cyber workforce.

Research Grants Awarded

CCI awarded and funded 18 grants to CCI research teams throughout the commonwealth. The CCI Hub funded 9 grants. The Northern Virginia Node funded 1 additional grant, the Coastal Virginia Node funded 4 additional grants, and the Southwest Virginia Node funded 1 additional grant. Additionally, the Southwest Node and Coastal Node split funding for 1 grant, and the Northern Node and Coastal Node split funding for 1 grant. The number and value of grants associated with each CCI Node are tabulated in Figure 2.2 and Figure 2.3. Individual grants are listed in Appendix 2.

Node	Number of Grants	Grant Total
Central Virginia	3	$300,000
Coastal Virginia	3	$300,000
Northern Virginia	1	$100,000
Southwest Virginia	2	$200,000
Total	**9**	**$900,000**

Figure 2.2: AI for Cybersecurity / Cybersecurity for AI Research Projects - Hub Funded.

Node	Number of Grants	Grant Total
Coastal Virginia	4	$400,000
Northern Virginia	1	$100,000
Southwest Virginia	1	$100,000
Shared – Northern & Coastal	1	$100,000
Shared- SWVA & Coastal	2	$200,000
Total	**9**	**$900,000**

Figure 2.3: AI for Cybersecurity / Cybersecurity for AI Research Program - Node Funded.

2.2.2 Node Funded Research Projects 2025

In FY25, the CCI Regional Nodes awarded and funded 36 research programs totaling $1,984,460 in research grants. The research projects are focused on a wide range of cybersecurity topics, such as supply chain security, artificial intelligence, smart technologies, Internet of Things, autonomous systems, wireless network security, and 6G. Additionally, numerous projects are multi-disciplinary and are collaborative efforts with research teams from several universities in Virginia. A detailed description of the Node research projects is below:

2.2.3 Central Virginia Node

Title of the Research Program:

CVN Research Grant FY25

Objective of the Call:

Fund CCI-related research in CVN institutions. As the CVN leader, VCU uses CCI funding to strengthen a robust research program and seeks to support projects related to CVN's research focus areas: cyber-physical systems, autonomous systems, Internet of Things (IoT), as it applies to medical device security, and smart city technology. This CCI-funded program aims to fund projects that relate directly to CCI's overall mission and CVN's research focus areas, producing novel research.

Selection Criteria:

The applications received in response to this RFP will be evaluated by a panel of reviewers and scored according to the following criteria:

- Strong intellectual merit related to CCI's mission
- Strong broader impacts related to CCI's mission
- Relevance to industry needs
- Potential to generate additional funding and revenue
- Strong relevance to CVN's focus areas

Research Grants Awarded: 11

The number and value of grants are listed in Figure 2.4. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
Virginia Commonwealth	2	$200,000
University of Virginia	8	$650,000
Virginia State	1	$100,000
Total	**11**	**$950,000**

Figure 2.4: FY25 - Central Virginia Node Research Projects.

2.2.4 Northern Virginia Node

Title of the Research Program: Research in Artificial Intelligence and Cybersecurity

Focus of the Call:

The focus of this call for proposals is to advance the state of the art of artificial intelligence (AI) and/or cybersecurity for AI. Topics include, but are not limited to:

- Anomaly detection
- Automated cyber defense
- System integrity automation
- AI assurance as it relates to cybersecurity
- Machine Learning (ML) integrity
- Enhancements to the resiliency of open-source AI and ML platforms to cyberattacks
- Explainability of security measures in automated cyber systems

Objectives of the Call:

The funded projects leverage NoVa Node funds and are open to Principal Investigators (PIs) in any of the public institutions that are part of CCI NoVa Node.

- To produce seminal contributions to artificial intelligence as related to cybersecurity, targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources

- To produce research contributions that benefit Virginia companies
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) in supply chain cybersecurity

Selection Criteria

Each proposal was reviewed by at least three subject matter experts and evaluated according to the following criteria:

- Strong intellectual merit related to cybersecurity
- Relevance to the focus of the call on AI and cybersecurity
- Clear plan for obtaining additional funding from government, private sector, philanthropy, etc., and likelihood of being competitive for the programs identified by the PI
- Strong broader impacts related to CCI's mission lines of innovation and workforce development, as well as in diversifying the cyber workforce

Research Grants Awarded: 2

The number and value of grants are listed in Figure 2.5. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
George Mason University	2	$150,000
Total	2	$150,000

Figure 2.5: FY25 - Northern Virginia Node Research Projects.

2.2.5 Southwest Virginia Node

Title of the Research Program

FY25 Cybersecurity Research

Objective of the Call:

The Cybersecurity Research Program exists to fuel major research thrusts, furthering CCI's role in a commonwealth-wide ecosystem of innovation excellence in cybersecurity. Focus areas are within the intersection of data, autonomy, and security. The CCI Southwest Node has a particular emphasis on cybersecurity related to fast, secure, and customizable communications systems and technologies, including 5G, artificial intelligence (AI), machine learning (ML), defense-in-depth cybersecurity solutions, emerging technologies (such as NextG and quantum information science, technology, and engineering) and cryptographic protocols, applications in transportation, energy, space, autonomous systems, manufacturing, agriculture, and healthcare, as well as issues surrounding human factors, privacy, ethics, and global security in society. CCI is interested in research that may lay the foundation for startups or spinouts in the cybersecurity sector.

Selection Criteria

Proposals were evaluated by a panel according to the following criteria:

- Intellectual merit (40%)

- 1. Clearly defined problem/unmet need
- 2. How the proposed work will address it
- Broader impacts (20%)
- 1. Potential to benefit society, including talent development
- 2. Contributions to the achievement of specific, desired societal outcomes, as aligned with the CCI mission
- Value of funding (20%)
- 1. Concrete plans to use the results from this research to secure external funding or IP
- 2. Concrete plans to use the results from this research to secure IP
- Alignment and qualifications (20%)
- 1. Relevance to CCI mission
- 2. Suitability of the team for the proposed work

Research Grants Awarded: 15

The number and value of grants are listed in Figure 2.6. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
Virginia Tech	15	$680,000
Virginia Military Institute		$37,500
Total	**15**	**$717,500**

Figure 2.6: FY25 - Southwest Virginia Node Cybersecurity Research Program.

Title of the Research Program

FY25 Global Engagement

Objective of the Call

The CCI Global Engagement Program exists to fuel major research thrusts via diverse approaches and teams, furthering Virginia's reputation as a leader in cybersecurity through international activities. Examples of potential projects include collaborative research visits, working groups, workshops, partnership development, and student internships. Investigators are encouraged to consider creative approaches to international engagement that advance discovery and application, cultivate ties for high-impact scholarship or large-scale proposal efforts, integrate approaches, widely disseminate results, or promote global training in cybersecurity. Focus areas should be within the intersection of data, autonomy, and security.

Selection Criteria

Proposals were evaluated by a panel according to the following criteria:

- Intellectual merit (40%)
- 1. Clearly defined problem/unmet need
- 2. How the proposed work will address it

- Broader impacts (20%)
- 1. Potential to benefit society, including talent development
- 2. Contributions to the achievement of specific, desired societal outcomes, as aligned with the CCI mission
- Value of funding (20%)
- 1. Concrete plans to use the results from this research to secure external funding or IP
- 2. Concrete plans to use the results from this research to secure IP
- Alignment and qualifications (20%)
- 1. Relevance to CCI mission
- 2. Suitability of the team for the proposed work

Research Grants Awarded: 5

The number and value of grants are listed in Figure 2.7. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
Virginia Tech	3	$30,000
Radford University	1	$9,628
University of Virginia-Wise	1	$10,000
Total	**5**	**$49,628**

Figure 2.7: FY25 - Southwest Virginia Node Global Engagement Program.

Title of the Research Program

Security Scholars Program

Objective of the Call

This program is designed to address the need for cost share from the faculty member or institution to gain a larger award. This type of commitment is usually a year of funding for a graduate research assistant for the entirety of the research project.

Research Grants Awarded: 3

The SWVA Node awarded 3 grants. Two grants were for the full support of a graduate research assistant for 2 ongoing projects. The other was for the support of a student for a semester. The number and value of grants are listed in Figure 2.8. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
Virginia Tech	3	$117,332
Total	**3**	**$117,332**

Figure 2.8: FY25 - Southwest Virginia Node Security Scholars Program.

2.2.6 CCI Fellows Program 2025

This program, launched in Fiscal Year 2022 (FY22), has the objective of supporting large-scale proposals for extramural funding involving two or more CCI institutions. Increasing the competitiveness of our researchers to obtain funding for center-scale projects is one of our strategic goals.

Objective of the Call

This call funds CCI researchers to lead center-scale proposals. PIs funded under this call are designated as CCI Fellows. Proposals must involve at least two CCI institutions of higher education (from any Node). A CCI institution of higher education must play a coordination role in the project. The budget associated with CCI institutions in the center-scale proposal must be at least $2 million.

Proposals must be in response to a published call or a direct solicitation from a funding agency or company.

This program is funded with CCI Hub funds, and receives proposals on a rolling basis. The program was announced in early 2022, and the first awards happened in Fiscal Year 2023 (FY23).

Selection Criteria

Proposals are evaluated by peer reviews and a final determination on funding is made by the CCI leadership according to the following criteria: strong intellectual merit relevant to CCI's mission and to the topic of this call, strong broader impacts related to CCI's mission, competitiveness of the team for center-scale funding, and potential to generate additional funding and revenue. The FY25 CCI Fellows are pictured in Figure 2.9a and Figure 2.9b; they join three Fellows funded in FY24 and six funded in FY23.

Dr. Dong S. Ha, from VT, is a FY25 CCI fellow who leads a proposal titled, "Embedded Wireless Security Through Quantum-Driven Topological Antennas," with two co-PIs from VCU and VT. He proposes leveraging the unique quantum properties of topological insulators (TIs) to achieve highly secure wireless communication. By submitting this research proposal to the NSF Growing Convergence Research (GCR) program, Dr. Ha envisions a transformative paradigm shift in wireless security by harnessing the quantum properties of topological insulators. This innovation aims to revolutionize secure communication systems, addressing critical vulnerabilities in emerging technologies such as healthcare, Internet of Things (IoT), and critical infrastructure. The proposed center will act as a Hub for pioneering research, focusing on secure wireless communication for Unmanned Autonomous Vehicles (UAVs), including drones and ground vehicles. Additionally, the project will serve as a critical workforce development engine, training a new generation of scientists and engineers in quantum materials, RF systems, and secure communication technologies.

Dr. Abhishek Phadke, from Christopher Newport University (CNU), is a FY25 CCI fellow leading a proposal titled, "Ensuring System Integrity in Smart Grids: Automation of Cybersecurity Protocols using AI for Continuous Monitoring and Response" with a team of four from CNU and ODU. This AI-backed response system will be designed to adapt, rebound, extend, and withstand malicious interaction with the grid. Fuzzily described as "system resilience," real-world systems have struggled to achieve this property. Dr. Phadke and his team plan to apply to the NSF Energy, Power, Control, and Networks (EPCN) program. He also plans on organizing a node-wide hackathon, creating and demonstrating a center-scale training program, partnering with Dominion Energy and Tarus NuEnergy to host a summer workshop on industry adoption and needs gathering in the energy sector, and then transitioning the research with industry partners to federal programs.

2.3 Faculty Recruited

2.3.1 Hub Faculty

The CCI Hub hired one post-doctoral researcher in FY25:

Dr. Nazmul Sikder Dr. Sikder is a researcher focused on artificial intelligence, cybersecurity, and cyber-physical systems. His work aims to build trustworthy AI models for critical infrastructure, especially water and wastewater systems. He developed methods for anomaly detection, forecasting, and soft sensing using deep learning, generative models, and causal inference. He completed his Ph.D. in Computer Engineering at

(a) Dr. Dong S. Ha

(b) Dr. Abhishek Phadke

Figure 2.9: FY25 CCI Fellows.

Virginia Tech in 2024. Earlier, he earned an M.S. from Virginia Tech in 2022 and his B.Sc. in Electrical and Electronic Engineering from BUET in 2015. His research focus includes developing hybrid neural networks that combine domain knowledge and contextual data to improve prediction accuracy in real-world systems. He has published in journals such as ACM Transactions on Cyber-Physical Systems and IEEE Access. Before graduate school, he worked at Grameenphone for four years, where he built data analytics tools to optimize network operations. These tools improved team efficiency and helped reduce costs. He received multiple awards for innovation and impact. Currently, he is preparing an NSF proposal focused on secure and resilient AI for infrastructure. He is especially interested in combining cyber, physical, and environmental data for early threat detection. He enjoys solving real-world problems, mentoring students, and working on interdisciplinary teams to make AI safer and more useful.

Figure 2.10: Dr. Nazmul Sikder.

2.3.2 Node Faculty

2.3.3 Northern Virginia Node

Dr. Umit Karabiyik was recruited to George Mason University as part of its efforts to continue to scale our ability to meet the educational demand from students interested in pursuing cybersecurity degrees.

Dr. Karabiyik's responsibilities in his role as a CCI Fellow will include:

- Assisting in interdisciplinary and industry-academia collaborative research efforts of both the Northern Virginia Node and broader Commonwealth Cyber Initiative ecosystems
- Leverage university-level strategic priorities in cybersecurity research to lead transformative growth and impact the research portfolio, and to further encourage and foster new and existing collaborations with academic, industrial, and governmental institutions in Northern Virginia and the greater Washington, D.C. region

- Accelerate the growth of high-quality academic programs, facilitate interdisciplinary research initiatives, and broaden the scope and focus areas of research in Mason with significant potential for commercialization

Dr. Karabiyik received his Bachelor's degree in Computer Systems Teaching from Sakarya University, and his Master's and Ph.D. in Computer Science from Florida State University. Dr. Umit Karabiyik was an Associate Professor in the Computer and Information Technology Department at Purdue University. Prior to his appointment at Purdue, Dr. Karabiyik was an Assistant Professor in the Department of Computer Science at Sam Houston State University from 2015 to 2018. He has secured federal and industrial funding from the U.S. National Institute of Justice, U.S. Department of Homeland Security, U.S. Federal Emergency Management Agency, U.S. Bureau of Justice Assistance, The National Air and Space Intelligence Center (NASIC), and Lockheed Martin Corporation. He is an Editorial Board Member of Springer Nature's Discover Computing journal, the Journal of Surveillance, Security and Safety, and conference chair and/or technical program committee member of high-quality international conferences in Digital Forensics, Cybersecurity, and Networking. Dr. Karabiyik's research interests include Digital Forensics, Cybersecurity, Forensic Intelligence, User and Data Privacy, Artificial Intelligence in Security, Privacy, and Forensic Applications.

Figure 2.11: Dr. Umit Karabiyik.

2.3.4 Southwest Virginia Node

Dr. Sarah Arpin; Assistant Professor Dr. Arpin is currently an Assistant Professor in Virginia Tech's Math Department. Dr. Arpin completed her postdoctoral research at Universiteit Leiden and the Quantum Software Consortium under Dr. Peter Bruin from 2022 to 2024. Additionally, she earned her PhD in Pure Mathematics from the University of Colorado Boulder, under the guidance of Dr. Katherine E. Stange, and also holds a Certificate in Data Science Statistics from CU Boulder. Dr. Arpin's research focuses on algebraic number theory and post-quantum cryptography, including the study of supersingular elliptic curves, isogeny-based cryptography, arithmetic geometry in characteristic p, and code-based cryptography.

Dr. Christiana Charmon Garcia; Assistant Professor Dr. Christiana Chamon's research interests encompass a wide range of topics, including noise-based authentication, decentralized identity, cyber-physical systems, security in artificial intelligence, engineering education, human-computer interaction, accessibility in engineering and kinesiology, and exercise science. Her accomplishments include serving on the Advisory Board for Unsolved Problems on Noise (UPoN 2024), being part of the Admissions Committee at Texas A&M University (TAMU) for 2023-2024 and receiving the FFDP Fellowship from Virginia Tech in 2023. She also served on TAMU's Scholarship Committee in 2022-2023 and was awarded the Ebensberger Fellowship in 2021. Dr. Chamon's teaching interests include circuits, electronics, cybersecurity, and control systems.

Dr. Murat Kantarcioglu; Professor Dr. Murat Kantarcioglu is a professor in the Computer Science department and a CCI Faculty Fellow. His research interests include data and artificial intelligence, security and privacy, and blockchain data analytics. He earned his Ph.D. in Computer Science from Purdue University in 2005, where he also received a Graduate Certificate in Applied Statistics. Prior to that, he completed a

B.S. in Computer Engineering with a minor in Finance from Middle East Technical University in Ankara, Turkey, in 2000.

Dr. Efat Fathalla; Assistant Professor Dr. Efat Fathalla is an Assistant Professor in the Department of Electrical and Computer Engineering at the Virginia Military Institute, USA. She earned her Ph.D. in 2024 from Old Dominion University, USA. Her research interests include privacy-preserving technologies, blockchain applications, the Internet of Things (IoT), and cryptography. Efat has worked on several research projects focusing on security in both the physical and application layers of communication systems. She has authored multiple patents, book chapters, journal publications, and papers presented at esteemed conferences.

Dr. Eduardo Camps Moreno, Presidential Postdoctoral Associate Dr. Camps Moreno's research interests include coding theory and quantum error-correction. He was a visiting scholar at Cleveland State University before his post-doctoral appointment at Virginia Tech. He earned his Ph.D. in 2023 from the National Polytechnic Institute of Mexico, where he also received a Master of Science and undergraduate degrees in mathematics and physics.

Dr. Chen Bai, Presidential Postdoctoral Associate Dr. Chen Bai has research interests in post-quantum cryptography. His research mainly focuses on provable security against quantum attacks. He received his Ph.D. from the Joint Center for Quantum Information and Computer Science (QuICS) at the University of Maryland, College Park. He was advised by Jonathan Katz and Gorjan Alagic.

Dr. Bahman Abolhassani, Presidential Postdoctoral Associate Dr. Bahman Abolhassani's research centers at the intersection of data, security, and autonomy, with a special use case of open radio access networks (O-RAN) and 6G/Next-G. He received his Ph.D. from The Ohio State University in Electrical and Computer Engineering. He also received master's and bachelor's degrees from Sharif University.

Dr. Raveendra Babu Ponnuru, Postdoctoral Associate Dr. Raveendra Babu Ponnuru has research interests in cryptography and information security. He earned his Ph.D. from the National Institute of Technology, Andhra Pradesh, India. His academic advisor was Dr. Alavalapati Goutham Reddy.

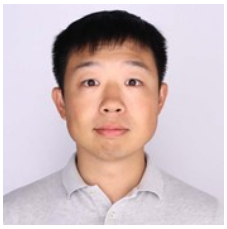
(a) Dr. Sarah Arpin

(b) Dr. Christiana Charmon Garcia

(c) Dr. Murat Kantarcioglu

(d) Dr. Efat Fathalla

(e) Dr. Eduardo Camps Moreno



(f) Dr. Chen Bai

(g) Dr. Bahman Abolhassani

(h) Dr. Raveendra Babu Ponnuru

Figure 2.12: Southwest Node New Faculty

2.4 CCI xG Testbed

CCI has made a major investment in creating a geographically distributed testbed for research and innovation in 5G and Next Generation networks. We call it the *CCI xG testbed*. This platform is allowing CCI researchers, in partnership with government and industry, to experiment, validate, and test new technologies

and approaches to accelerate fundamental research and innovation on cybersecurity in the context of the next generation of mobile and fixed networks.

In FY25, CCI's xG testbed has continued to expand, with new indoor xG testbed equipment, provided in kind, to support the ACCoRD project, and continued building and testing to support outdoor deployment in Blacksburg, VA.

Value Proposition

The xG Testbed contains assets for research and innovation in 5G and NextG, embedding Artificial Intelligence (AI) in the operation of the network, supporting research in network security, Open Radio Access Network (O-RAN) security, and AI assurance, among other topics. Figure 2.13 shows the logo developed for the testbed.

Figure 2.13: CCI xG Testbed logo.

The value proposition for the xG Testbed can be summarized as follows:

- First end-to-end ORAN-compliant 5G/6G network with fully integrated AI infrastructure. Fully built with open source AI and network components.
- Includes massive computing and storage capabilities, focusing on AI Assurance for cybersecurity.
- This multi-site testbed allows experimentation with non-locality in complex networks.
- Able to deploy at scale AI solutions in distributed networks.
- Supports hands-on multi-disciplinary training of cyber professionals well-versed in AI and communications.

Design Principles

Our goal is to support innovation that is aligned with the standardization of 5G being led by the 3rd Generation Partnership Project (3GPP) as well as to contribute to the emerging vision for the next generation of networks, which we refer to as *Next G*. To this end, we adopt the following principles in the design of our testbed:

- Openness: reliance on open systems, whenever possible, for access to communications and network functions and programmability;
- Accessibility: access to the testbed by researchers throughout the CCI network of institutions;
- Programmability: configurable and programmable hardware and source, end-to-end, from the user equipment to the core network;

- Flexibility: flexible network management and orchestration compliant with an end-to-end 5G architecture composed of a mix and match of open-source and commercial hardware and software, with a cybersecurity focus, enabling indoor and outdoor deployment;
- Componentization: fully componentized implementation with open Application Programming Interfaces (APIs); containerized, cloud-ready implementations;
- Interoperability: integration ensuring the integrity of the end-to-end solution; interoperability among network components and existing testbeds, securing and hardening the network infrastructure;
- Support of verticals: alignment with key verticals to be supported by 5G and Next G networks, and co-location with research infrastructure supporting those verticals.

The testbed has components located in the CCI Hub and each of the Nodes. These components are aligned with verticals that are of particular focus in each node: national security, autonomous vehicles, transportation networks, manufacturing and supply chain in the NoVA Node; Internet of Things (IoT), smart communities, and medical devices in CVN; ports and warehouses in the CoVA Node; autonomous and unmanned vehicles, additive manufacturing, and the energy grid in the SWVA Node. The testbed component in the CCI Hub provides a full-stack 5G core and radio access network, including commercial-grade and experimental Software Defined Radio (SDR) equipment and open source software; it is accessible remotely by all CCI researchers.

2.5 Research Highlights and Breakthroughs

CCI researchers across the state are advancing the cybersecurity field at a fast clip, as our third annual Research Paper Showcase demonstrates. The peer-reviewed published papers are based on CCI-funded research and acknowledge CCI's contribution in the paper.

In FY25, 18 selected papers cover such topics as AI for Cybersecurity/Cybersecurity for AI, Cyberattack Resilience, Cybermanufacturing Security, Cryptography, and Wireless Security. The showcase features researchers from ODU, University of Virginia (UVA), VCU, VT, William & Mary (W&M), and industry, as well as national and international universities.

Learn more about the Research Paper Showcase.

AI for Cybersecurity/Cybersecurity for AI

CryptoPUF: A Lightweight and ML-Resilient Strong PUF Based on a Weak PUF and Crypto Core. Authors: Yimin Gao, John Chilaka, Elisa Pantoja, Robert Klenke, Mircea Stan

Hermes: Boosting the Performance of Machine-Learning-Based Intrusion Detection System through Geometric Feature Learning.Authors: Chaoyu Zhang, Shanghao Shi, Ning Wang, Xiangxiang Xu, Shaoyu Li, Lizhong Zheng, Randy Marchany, Mark Gardner, Y. Thomas Hou, Wenjing Lou

OSINT Clinic: Co-designing AI-Augmented Collaborative OSINT Investigations for Vulnerability Assessment.Authors: Anirban Mukhopadhyay, Kurt Luther

SPOT: Structure Patching and Overlap Tweaking for Effective Pipelining in Privacy-Preserving MLaaS with Tiny Clients. Authors: Xiangrui Xu, Qiao Zhang, Rui Ning, Chunsheng Xin, Hongyi Wu

Cybermanufacturing Security

BioSaFe: Bioprinting Security Framework for Detecting Sabotage Attacks on Printability and Cell Viability. Authors: Muhammad Ahsan, Eunice Pak, Kate Jackson, Muhammad Haris Rais, Barry Najarro-Blancas, Nastassja Lewinski, Irfan Ahmed

Cryptography

Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations. Authors: Efat Fathalla, Mohamed Azab

Breaking barriers in two-party quantum cryptography via stochastic semidefinite programming. Authors: Akshay Bansal, Jamie Sikora

CSI-Otter: isogeny-based (partially) blind signatures from the class group action with a twist. Authors: Shuichi Katsumata, Yi-Fu Lai, Jason T. LeGrow, Ling Qin

Resilience to Cyberattacks

CTINEXUS: Automatic Cyber Threat Intelligence Knowledge Graph Construction Using Large Language Models. Authors: Yutong Cheng, Osama Bajaber, Saimon Amanuel Tsegai, Dawn Song, Peng Gao

An Exploratory Mixed-methods Study on General Data Protection Regulation (GDPR) Compliance in Open-Source Software. Authors: Lucas Franke, Huayu Liang, Sahar Farzanehpour, Aaron Brantly, James C. Davis, Chris Brown

Principled and Automated Approach for Investigating AR/VR Attacks. Authors: Muhammad Shoaib, Alex Suh, Wajih Ul Hassan

Security Enhancement in UAV Swarms: A Case Study Using Federated Learning and SHAP Analysis. Authors: Sushmitha Halli Sudhakara, Lida Haghnegahdar

Scale-MIA: A Scalable Model Inversion Attack against Secure Federated Learning via Latent Space Reconstruction. Authors: Shanghao Shi, Ning Wang, Yang Xiao, Chaoyu Zhang, Yi Shi, Y. Thomas Hou, Wenjing Lou

S2M3: Split-and-Share Multi-Modal Models for Distributed Multi-Task Inference on the Edge. Authors: JinYi Yoon, JiHo Lee, Ting He, Nakjung Choi, Bo Ji

"This is not a scam!": Assessment of an awareness-raising program tackling older adults' scam victimization in a multi-method study. Authors: Katalin Parti, Sophia Silis, Pamela Teaster, Susanna Rinehart, Charles Dye

Unraveling the Complexities of MTA-STS Deployment and Management in Securing Email. Authors: Md. Ishtiaq Ashiq, Tobias Fiebig, Taejoong Chung

Wireless Security

Managing O-RAN Networks: xApp Development From Zero to Hero. Authors: Joao F. Santos, Alexandre Huff, Daniel Campos, Kleber V. Cardoso, Cristiano B. Both, Luiz A. DaSilva

Out-of-Band Interference Management to Protect Radio Astronomy (Dr. Vanu Bose Best Paper Award Winner). Authors: Naru Jai, Yi Shi, Wenjing Lou, Luiz A. DaSilva, Y. Thomas Hou

Chapter 3

CCI Workforce Development

CCI has invested in creating new experiential learning opportunities for Virginia students, and in pairing students with cyber startups, medium and large businesses, and government agencies for training and career development opportunities. This chapter highlights the CCI programs that focus on workforce development.

3.1 Hub-Led Programs

3.1.1 CCI Internship Fair

The CCI Internship Fair took place in late September 2024 and proved again to be one of our most popular programs. Over 400 students from over 30 different institutions of higher education registered for this free and virtual event featuring representatives from a variety of employers ranging from government agencies to Virginia-based companies. Featured employers included: Naval Surface Warfare Center Dahlgren, Defense Intelligence Agency, G@OPS, BroadFuture, City of Newport News, Cyberteck Academy, and CTEWorkforce.

3.1.2 CyberFusion

The Commonwealth Cyber Fusion, hosted by VMI, Senator Mark R. Warner, the Virginia Cyber Range, and CCI took place on the VMI campus on February 21-22, 2025. The invitation-only event is for colleges that are National Security Agency (NSA) / Department of Homeland Security (DHS) designated National Centers of Academic Excellence in Cyber Defense. CyberFusion combines a collegiate cyber competition with learning and career opportunities, featuring a career fair and the Virginia Cup Capture the Flag Competition. This year also featured a new event administered by TechDuels. Tech Duels features passionate participants debating technical topics in various formats, including one-on-one and team battles, competing for prizes and recognition. All debaters undergo training from seasoned coaches to refine their arguments, while judges and moderators are trained for effective evaluation and scoring. The event hosted two competitions, one for 4-year and one for 2-year colleges. 130 students from 18 colleges and universities competed over the weekend. Friday's activities included a keynote speech by Don Mills, Principal Architect for Cisco's Security and Trust Organization, and the TechDuels competition. This year's competition included 44 challenges, the most ever. The winners of the capture-the-flag-style Virginia Cyber Cup competition for the four-year college division are: James Madison University in first place, George Mason University in second place, and the University of Virginia in third place. For the community college division: Danville Community College in first place, Northern Virginia Community College in second place, and Germanna Community College in third place.

3.1.3 Project-based Learning Program

The CCI Project-Based Learning Program solicits projects from industry sponsors for students to work on for one or two semesters while being actively mentored by the industry sponsor. In FY25, CACI continued its commitment to Virginia students by hosting another cohort of students, this time from Old Dominion

University, Virginia Tech, and George Mason University. CCI added two new companies to the PBL portfolio in FY25: Guidepoint Security and Public Broadcast Service. Students working for Guidepoint Security created a "SOC-in-a-Box," which is a scalable and quickly deployable lab environment exposing students to technologies they will encounter as they enter the Cyber Security job market for crucial roles such as Incident Response Analyst, Threat Intelligence Specialist, Detection Engineer, and Adversary Emulation Specialist. Students working for the Public Broadcast Service completed a cyber-vulnerability assessment for their cyber division.

3.1.4 Clearance Preparedness Program

In FY25, the CCI Hub continued a virtual series to prepare students for the security clearance process, after two successful cohorts in FY23 and FY24 with over 400 students registering. This program, entitled "The Clearance Preparedness Program," includes ten virtual webinars ranging in topics from "What is a security clearance and why would I want one?" to "Common reasons people do not pass a clearance process." Students from across CCI are eligible to participate, and if they attend 80 percent of the modules, they will earn a digital badge signaling that they are informed about and prepared to begin a security clearance process. The modules are hosted by CCI's Dr. Eric Burger and feature representatives from industry and government discussing various aspects of security clearances. Looking forward to 2026, the program is undergoing a revamp, which will feature sessions twice a month, and students will be able to complete all the modules within the Spring 2026 semester.

3.1.5 Experiential Learning Program in FY25

The Experiential Learning Program is CCI's longest-running program, with the FY25 batch of awards being the sixth time CCI has run this program. In its sixth iteration, the 2025 Experiential Learning call for proposals elicited 28 submissions, with eight successful proposals totaling $723,567 awarded in grants. CCI researchers were eligible to respond to this call, and proposals were selected based on recommendations by a peer review group. The percentage of the funding for projects in each CCI Node is shown in Figure 3.1.

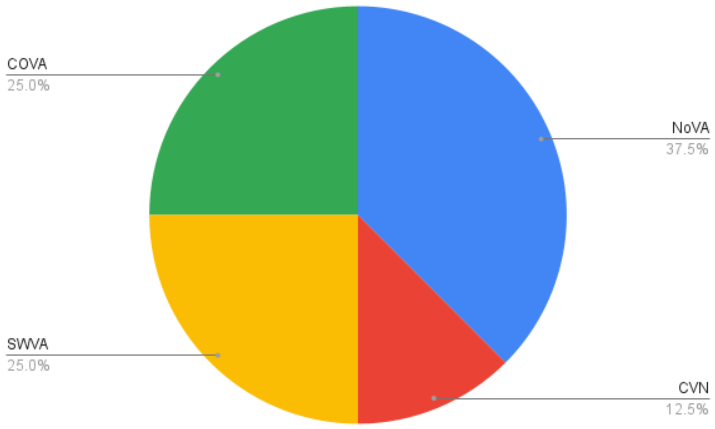


Figure 3.1: Funding percentage by Node for the FY25 Experiential Learning program.

The projects funded by this program are summarized below.

- **Cybersecurity Field Training Experience**: Liza Wilson-Durant; Mason. There are approximately 51,000 cybersecurity job openings in Virginia, and the existing pipeline of cybersecurity-related degree-seeking candidates is not enough to fill the demand. New sources of talent, including those with degrees outside of the typical cybersecurity pathway, but with hands-on skills developed in the field, present a viable source to meet this demand. This Cybersecurity Field Training Experience (C-FTE) seeks to tackle this problem on two distinct fronts. The C-FTE will pair graduate student subject

matter experts and project supervisors with a pair of undergraduate students and place each team with an industry or government partner. Under this arrangement, graduate students will serve as the primary source of technical expertise, sharing their knowledge with undergraduates and guiding them through project tasks. This program will also enable the exposure of less cybersecurity-oriented undergraduate majors (e.g., IT, math, business) to cybersecurity skills and knowledge, and even acquire technical cybersecurity skills. During the C-FTE, undergraduate students will develop the technical capacity needed to set them up for entry-level cybersecurity jobs, and graduate students will develop the technical leadership skills required of early mid-level managers in the cybersecurity workforce.

- **Cyber Startups**: Gisele Stoltz; Mason. Building on the successes of the previous five years of iterations of the CCI Experiential Learning Programs, this proposal aims to enhance the existing program and strengthen our collaborations with the University of Mary Washington and James Madison University, which were added last year to the program. Experiential learning plays a vital role in equipping students for careers in the cybersecurity field. The technical and interpersonal skills that technology employers seek are increasingly difficult to acquire through conventional college programs and standard internships. The challenge is further exacerbated by the limited number of internship opportunities available since many positions require security clearances, which narrows the pool of qualified candidates. This poses a significant obstacle for undergraduate students who are aiming for valuable internships. Moreover, startups and small businesses struggle to attract skilled students, as they often compete with larger corporations and government organizations for the same talent in their regions. Recognizing the vital role that startups and small businesses play in the evolving Virginia cybersecurity landscape, the proposed project sets out to accomplish three key objectives. First, to equip students enrolled in cybersecurity degree programs with valuable, hands-on, experiential paid internships, while offering them mentorship and training. Second, to supply cybersecurity startups and small to medium-sized enterprises (SMEs) with the skilled talent necessary for business growth. Third, to expose students from diverse backgrounds to technology entrepreneurship, fostering an environment where some may consider launching their startups in the coming years.

- **Cybersecurity for Industry 4.0: A Multi-insitutional Camp for Cyber Workforce Readiness**: Christiana Chamon Garcia, VT; Nicole Akers VT; Benjamin Standfield; Virginia State University (VSU). The growing adoption of Industry 4.0 technologies in manufacturing has created critical vulnerabilities in interconnected systems, including IoT sensors, SCADA networks, and automated production lines. Industry 4.0 refers to the use of advanced digital technologies like IoT, automation, and data analytics to create smart, interconnected manufacturing systems. With manufacturing representing 26% of all cyber incidents, there is a distinct need for specialized workforce development. The proposed project addresses this need through an innovative week-long experiential learning program designed to train 30 students from Virginia Tech, Virginia State University, New River Community College, and Central Virginia Community College in manufacturing-specific cybersecurity skills. The program will employ Extended Reality Capture the Flag (XR CTF) exercises that simulate real cyberattacks on smart factory environments, providing participants with practical, hands-on experience responding to Industry 4.0 security threats. Through a structured curriculum featuring workshops, hands-on projects, and industry networking opportunities, students will develop workforce-ready skills while establishing connections with local industry members. The multi-institutional collaboration leverages expertise from academic institutions and industry partners, including GENEDGE, Boeing, and HUB Corporation. This initiative not only addresses immediate workforce needs but also establishes a scalable model for cybersecurity education that can be adopted across Virginia, ultimately strengthening the protection of critical infrastructure and positioning the commonwealth as a leader in cyber workforce development.

- **Enhancing the Incoming Cybersecurity Workforce Through Leveraging the Professional Readiness Experiential Program (PREP)**: Brian K. Ngac, Mason; Nirup Menon, Mason. This project seeks to scale and enhance George Mason University's Professional Readiness Experiential Program (PREP) to prepare students for the cybersecurity workforce. Through partnerships with industry participants such as FWI, Maximus, and Mobius, PREP will provide 30 northern Virginia-based college students with hands-on, agile, and industry-led cybersecurity projects. These students will gain

technical experience, develop client-facing communication skills, and engage in networking, mentorship, and specialized training. PREP's established methodology supports iterative improvement, interdisciplinary collaboration, and flexible project execution across academic semesters. The initiative aligns with the Commonwealth Cyber Initiative's (CCI) objectives in education, innovation, and workforce development, and will continue PREP's proven track record of student publications, cross-institution participation, and successful transitions into the cybersecurity field. Specifically, our industry participants' committed cost-share contributions totaling $24,000 further underscore their point of view of the program's importance and impact.

- **Expanding Experiential Learning Through the Commonwealth STEM Industry Internship Program Commonwealth STEM Industry Internship Program (CSIIP)**: Chris Carter; Virginia Space Grant Consortium (VSGC). This partnership serves the entire commonwealth and supports CCI's goal of cybersecurity workforce development. VSGC established CSIIP to support education, workforce development, and research by providing Virginia undergraduate students majoring in STEM with meaningful paid internships. The program is free to companies, schools, and students. CSIIP helps students explore career goals, apply classroom theory in the workplace, and develop their skills while working on real-world projects mentored by industry professionals. Since 2013, VSGC has placed more than 1,150 students, and several companies have hired their interns as full-time employees, including: Sentara, AScIS, Hampton Roads Sanitation District, RecAccess, Dominion Resource Services, MI Technical Solutions, BASF, York County, and City of Newport News.

- **Enhancing Experiential Learning via Technology Enabled Engagements with Mentoring (TEEM)**: AI-Enhanced Student Peer Mentoring; Jeff Pittges, Radford; Deri Draper-Amason, ODU; Bobby Keener, Civilian Cyber CEO/CIO. Virginia's higher education institutions equip students with academic knowledge, yet employer surveys consistently reveal a gap in graduates' readiness for the workforce, particularly in critical thinking, soft skills, and the practical application of theoretical learning. While experiential learning can address these gaps, many programs lack the structure needed for consistent, real-world impact. The Commonwealth Cyber Initiative (CCI) aligned Technology Enabled Engagements with Mentoring (TEEM) program provides structure to improve outcomes. In collaboration with hundreds of industry professionals, TEEM engaged hundreds of students across more than 20 Virginia higher education institutions and numerous K-12 school divisions. The proven TEEM approach delivers structured, student-led, experiential learning through high-impact mentoring emphasizing applied knowledge and entrepreneurial ideation. The AI-Enhanced Student Peer Mentoring project will further advance TEEM via the integration of a "Mentoring Insights AI-Assistant." For each mentoring session, transcripts will be captured and analyzed using a mentor AI Persona and a Cybersecurity-focused GPT (Generative Pre-trained Transformer). The proposed system will contextualize conversations using TEEM learning resources, curated web content, session agendas, feedback surveys, desired outcomes, and more. The AI-enhanced approach will provide enriched feedback for both mentees and mentors, including identification of learning gaps or misconceptions, suggested follow-up actions, engagement summaries, and extraction of novel insights (additional takeaways). The innovative use of AI enhances reflection, improves learning outcomes, and scales the impact of TEEM structured mentoring in cybersecurity education.

- **Network Forensics Workshop on Analyzing Cyberattacks in Industrial Control Systems**; Irfan Ahmed, VCU; Adeen Ayub JMU. This project aims to develop and organize a hands-on workshop and post-workshop challenge with the High Tech Crimes Division at Virginia State Police to investigate cyberattacks on industrial control systems (ICS) at a wastewater treatment plant. The participants will be introduced to network forensics in ICS environments, receive deep-dive training on ICS communication protocols, learn reverse engineering techniques for undocumented/proprietary protocols, and understand real-world ICS attacks through demonstrations and develop skills to detect them using network trace analysis. Water and wastewater treatment facilities in the United States have been subject to cyberattacks. This project will contribute to training a workforce that can investigate these attacks and solve cybercrime in a non-traditional ICS network environment.

- **Secure AI for Marine Ecosystems (SAME): Modeling Benthic Biomass with Image-Graph Fusion under Data Poisoning Threats**: Yi He, W&M; Daniel Runfola W&M; Roger Mann W&M.

We propose a new round of experiential learning that builds on a solid record from three prior CCI-funded initiatives, which have engaged 99 undergraduate students across the commonwealth in applied AI security research spanning satellite imagery, data poisoning, transportation systems, and maritime security. In collaboration with VIMS, NOAA, and the NSF, this new proposal will focus on securing AI systems designed to be leveraged by the fishing industry, focused on benthic biomass estimation. We propose hosting 25 students from multiple Virginia institutions, working closely with them in an experiential learning context to investigate how adversaries might leverage data poisoning to disrupt species detection and spatial ecological inference in image-graph fused AI systems. Students will design, test, and defend deep learning pipelines that combine HabCam imagery with graph neural networks to model marine species distribution, which is critical to fisheries monitoring and management in ecologically sensitive areas like the Chesapeake Bay. The program will continue to expand Virginia's cybersecurity talent pipeline while advancing foundational research in adversarial machine learning, contributing to national security, and supporting the commonwealth's long-term economic resilience.

3.1.6 Cyber As A Service

In FY24, the CCI Hub began a new program called Cyber As a Service in which projects, performed primarily by students, provide a cyber service (e.g., penetration or pen testing, cyber risk analysis) to Virginia small businesses or not-for-profits in the same county as the institution of higher education. This is an ongoing call for proposals with maximum grant awards of $15,000. In FY25, we continued this program, and one such funded project was awarded to Dr. Sherif Abdelhamid at VMI called "Student-led Cyber Defense: Creating a Safer Digital Landscape for Local Businesses and Non-Profits in Rockbridge County." In this project, VMI cadets will conduct comprehensive cybersecurity threat assessments, design and implement secure network systems, provide training, and offer advisory support for integrating artificial intelligence (AI) in customer acquisition, retention, marketing, and data analysis. These services are vital in the shared network environment at the Virginia Innovation Accelerator (VIA), where multiple entities rely on secure, individualized protections. The proposed project delivers essential cybersecurity services to VIA's tenants, and it serves as a valuable educational platform for VMI cadets, equipping them with hands-on experience in cybersecurity and network security. This initiative will enhance local organizational resilience and foster workforce readiness, benefiting the regional economy and the broader cybersecurity ecosystem.

3.2 Node-led Programs

In addition to the CCI-wide programs described above, in the past year, the CCI Nodes also developed and executed many successful workforce programs. Workforce development spending by the four CCI Nodes totaled $1,992,858.00 in FY25. The breakdown by Node is shown in Figure 3.2.

3.2.1 NoVA Node

CCI NoVa Node has made significant investments in workforce expansion by developing and funding experiential learning opportunities that not only expand the breadth of skills but also seek to expand the pipeline of cybersecurity expertise. By leveraging experiential learning to instill new skills in a new workforce that otherwise would not have access to robust learning opportunities, CCI NoVa Node is successfully widening the talent pipeline. In continued support of these efforts, CCI NoVa Node supported four (4) workforce initiatives during FY25:

- **High School Cybersecurity Internship Program**: CCI NoVa Node has scaled this program to support 45 high school students (seniors or just graduated) for internships with cybersecurity companies during Summer 2025. The experience includes a 2-week professional skills training program to prepare students for the professional work environment. This program represents a total of 12,150 student contact hours. 156 applications were received for the 45 available placements. Of the selected applicants, 47% identify as women and 56% come from underrepresented populations in science and engineering. Host companies include: Appian, BRICC, CGI Federal, Chainbridge Solutions, COSMIC, Deltek, GT Edge AI, Intelsat, Leidos, LoudounTec, ManTech, Maximus, NT Concepts, Obscurity Labs, Oceus

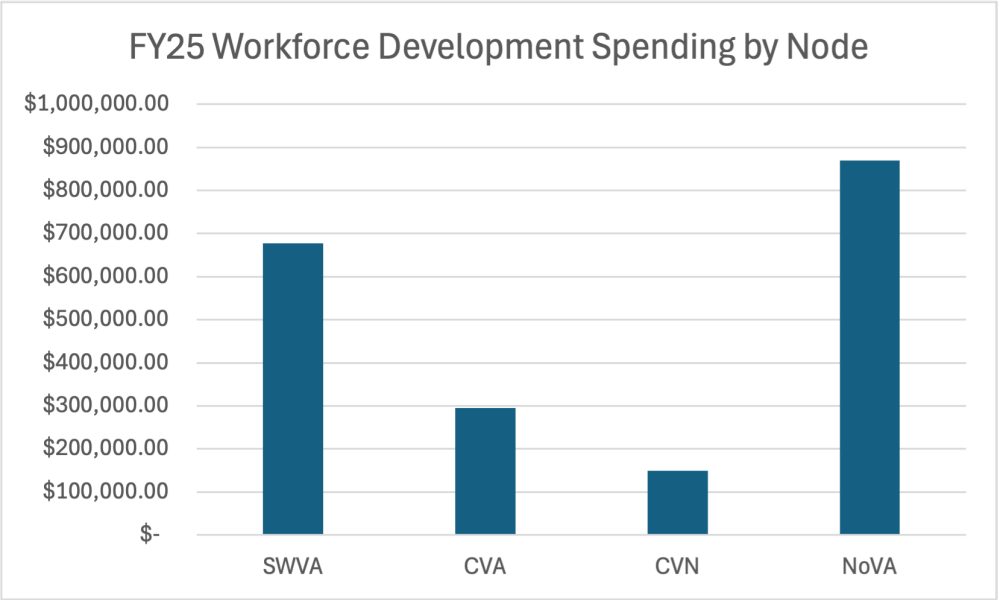


Figure 3.2: Workforce Development Spending by Node in FY25.

Networks, Solvitur Systems, Virginia Tech's Thinkabit Lab, Tyrula LLC, Unissant, and Widelity. This program is an expansion of the successful program launched in FY21 and scaled in FY22.

- **Undergraduate Research Program** CCI NoVA Node sponsored 44 undergraduate students conducting cybersecurity research at George Mason University, James Madison University, and the University of Mary Washington. Example research projects included:
  - An Exploration of LLM Development and Use in Open Source
  - Automated Detection of Inconsistencies in Interlinked Standards for Multi-Layer Complex Systems
  - Hardware Security for Autonomous Systems
  - Securing the Internet of Things (IoT) using AI Technologies
  - A Generative Approach to Side Channel Analysis-based Anomaly Detection
  - Uncovering Secrets from Virtual Reality Headsets via Electromagnetic Shields
  - Decentralized Machine Learning for O-RAN Systems
  - Companion Robot Cybersecurity
  - Security Research in Autonomous Automotive Vehicle Systems
  - Regional Cybersecurity Ecosystems

  These experiences are building significant technical expertise and capacity in undergraduates, making them particularly well trained for advanced work in industry and government. This program supported 16,075 student contact hours across FY25. Twenty-seven percent (27%) of this year's Undergraduate Research Assistants cohort identify as women, and 36% identify with underrepresented population groups in science and engineering.

- **Cybersecurity Traineeship Program**. As part of CCI NoVa Node's effort to expand the pipeline of cybersecurity talent beyond degree-seeking individuals, the CCI NoVa Node Cybersecurity Traineeship program is providing cybersecurity training and an immersive apprenticeship for people who wish to transition into a career in cybersecurity but do not have prior experience. This program includes a 7-week classroom learning and training experience, beginning June 9, 2025, followed by a 12-week

apprenticeship/traineeship with a cybersecurity company. The program received over 300 applications for 20 available positions. 45% of the cohort identify as female. Underrepresented population groups in science and engineering comprise 75% of this cohort.

- **Undergraduate Internship Program** This program enables undergraduates from across the CCI NoVa Node to participate in internships with cybersecurity companies from across the region. There are currently 32 students participating in this program, with more onboarding. Industry hosts include Auspex Labs, Blue Sky Innovations, Critical Shift, EngineeRD, Great Victory Legends, Rohic, RPRC, Solvitur Systems and TekScope. This program supported a combined 8,430 contact hours during FY25. Twenty-five percent (25%) of this cohort identify as female, and 44% identify with underrepresented population groups in science and engineering.

In addition to these dedicated programs, CCI NoVa Node enabled the widening of the talent pipeline through the support of external initiatives targeting high school students with an interest in a career in cybersecurity. NoVa Node supported CyberSlam 2025, which brought together members of the Secret Service, Homeland Security, high school teachers, George Mason University faculty, and more than 500 students from five counties and 22 high schools from the commonwealth to participate in a hands-on cybersecurity event. NoVa Node also served as a sponsor for PatriotHacks 2024, which attracted over 500 students to develop their technical capacity to address real-world problems presented by industry.

3.2.2 COVA CCI

CoVA CCI supports several programs in innovation, workforce development, and student experiential learning. These include the Innovate Cyber Challenge, Internships and the Cybersecurity Clinic.

- **Innovate Cyber Challenge**. COVA CCI completed another cohort of its Innovate Cyber Challenge in spring 2025 with a total of 41 students from six universities and colleges. These included Christopher Newport University, Northern Virginia Community College, Old Dominion University, the University of Virginia, Virginia Tech, and William & Mary. This program groups students into teams, and each team is assigned a cybersecurity problem/challenge. Over the semester, the teams use design thinking to produce unique solutions for the problem and present their final product during a Showcase event in April 2025. This year's challenge asked: How might we make cybersecurity more understandable, approachable, and encourage best practices around cybersecurity? The teams participating in this year's cohort are:
  - CyberQuest
  - Internet Explorers
  - MailSenti
  - No Fine Print
  - OASIS
  - PhishProof
  - PufferShield
  - Safety Mode
  - SecureXP
  - SpamLock
- **COVA CCI Internships**. One goal of CCI and COVA CCI is to grow the cybersecurity workforce in the commonwealth. COVA CCI is working with university researchers and business partners to achieve this goal. Old Dominion University, with support from COVA CCI, analyzed the School of Cybersecurity internship program. The School of Cybersecurity requires its Bachelor of Science students to complete an internship as part of the cybersecurity curriculum. This is accomplished by completing the CYSE 368, Internship Course. After gathering and analyzing data for the students who completed CYSE 368 since 2019, it was determined that 724 students completed an internship experience. COVA

CCI supported eighteen (18) interns for ODU's Center for Educational Innovation & Opportunity (CEIO) iLab. These students assisted CEIO by engaging with the diverse programming offered at the iLab and in executing hands-on STEM activities, such as field trips, family/community events, and outreach initiatives, by preparing materials, setting up equipment, and facilitating activities. Beyond event support, the interns contributed to the iLab's organizational tasks, including maintaining equipment, supporting program planning, and creating Coastal Virginia Center for Cybersecurity Innovation (COVA CCI), Southeastern Virginia's node of the Commonwealth Cyber Initiative (CCI) 17 marketing materials. Their involvement extended to collaborating with community partners and providing valuable administrative assistance, allowing the iLab to offer a wide range of enriching experiences for both youth and educators. Through their work, the interns gain practical experience in program delivery, technical skills, and project management, while making significant contributions to the iLab's success. During FY 2025, these 18 interns supported over 60 outreach events, including school field trips and community/family programs, connecting with over 560 students and members of the community.

- **COVA CCI Cybersecurity Clinic**. Starting with a pilot cohort in Spring 2024 semester, COVA CCI supported a Cybersecurity Clinic with eight (8) students from Old Dominion University, and two micro-businesses – a non-profit religious ministry and a government contractor. We partnered with Valor Cybersecurity, a local cybersecurity business, which provided training and subject matter expertise to the students as they prepared to assess the client's businesses. This program has continued to expand each semester. In fall 2024, we supported 15 students and four businesses, including the City of Suffolk, and in spring 2025, we supported 18 students and six companies. This clinic offers free cybersecurity-as-a-service to small businesses, non-profits, local government offices, agencies, and boards, as well as other organizations. Selected students to evaluate these organization's cybersecurity readiness and risk posture. The goal of this clinic is to raise cybersecurity awareness and to provide services such as education and risk management strategies to client organizations within Hampton Roads. It also offers students an experiential learning opportunity as cybersecurity interns/consultants. Specifically, this clinic targets those client organizations that lack a strong cyber presence and who can benefit from gaining cybersecurity knowledge through cybersecurity awareness initiatives and services. This is a 15-week program offered during the fall and spring academic semesters. During the program, students receive training on various cybersecurity modules, enabling them to interview client organizations beginning in the middle portion of the program. The students work in teams under the guidance of ODU faculty. The team provides service to the client in one or more areas of cybersecurity, including network defense, policies and procedures, cybersecurity training for employees, cyber risk assessments, and/or cybersecurity best practices. As of April 2025, ODU is a member of the Consortium of Cyber Clinics. The Consortium of Cybersecurity Clinics is an international network of university-based cybersecurity clinics and allies working to advance cybersecurity education for the public good.

3.2.3 SWVA Node

FY25 Workforce Grants from Appropriated Funds: Cybersecurity Workforce Grants The Cybersecurity Workforce Development Program exists to fuel major talent pipeline efforts that impact large numbers of students to address the cybersecurity workforce gap and increase the talent pool for cybersecurity positions. There was no formal process for this program, but workforce projects that were sent to the FY25 Cybersecurity Research call were considered.

Workforce Grants Awarded The SWVA Node awarded 4 grants. One project was a continuation of the Use and Abuse work that Dr. Alan Michaels has been working on for several years, which continues its streak of being able to engage students from broad ranges of academic backgrounds in applied cybersecurity research. The Professional Accelerated Cyber Education (PACE) program at Radford University aimed to strengthen cybersecurity workforce development in southwest Virginia. Through online, self-paced, competency-based training, PACE reached its target enrollment while aligning course content with industry needs. The program had 62 participants, with 16 earning certificates. The SWVA Workforce Engagement project engaged 188 participants in 5 different events, including a graduate and junior researcher summer school and collaborative workshop in Switzerland, a joint workshop in Bombay, India, an internship event engaging NIST and NSA researchers, Math Circles for K-12 outreach, and a MathCounts competition.

FY25 Securitas Living Learning Community Support The Securitas Living Learning Community (LLC) offers students an immersive experience centered on cybersecurity, leadership development, and community engagement. This inaugural year, students have taken part in a range of programs, including technical workshops, professional development events, peer-led Cyber Monday sessions, and social activities designed to build teamwork and networking skills. Highlights include the launch of Tech Horizons, a strengthened student leadership team, and increased student engagement across all programming. The LLC supported 46 undergraduate students.

FY25 Workforce Development Events

- **CCI SWVA Student Researcher Showcase:** In Southwest Virginia, hundreds of graduates and undergraduates are working in labs, internships or training programs that allow them to get hands-on with cybersecurity or engage in CCI research. These experiences equip students with highly specialized cybersecurity skills, preparing them to meet the growing demand for cybersecurity talent in the commonwealth and beyond. The CCI Researcher Showcase held on April 4, 2025, is an opportunity for the students to present their ongoing research projects and share their methods and results to date. We had over 30 undergraduate and graduate students present their work on electronic posters in 25 presentations. Awards were given for best poster, crowd favorite, and best technical presentation.

- **CCI SWVA Graduate Student Summit:** This workshop for graduate students is to provide a platform for sharing research objectives, approaches, and results. The objective of the presentation is to learn more about the problem the student is trying to solve, the progress they have made to date, the connection to security, and any results obtained. Work in progress is welcome, and final results are not necessary to present. The student presented their work, and all attending gave critical feedback to the student. This peer-to-peer feedback helps develop the presentation skills of the graduate student and helps them think about the progress of their research and research outcomes. The summit held on December 3, 2024, included 15 presentations.

- **Coding Theory and the Intelligence Community: Dive in!:** This event, held September 4, 2024, featured a talk by the National Security Agency Applied Mathematician Genevieve Maalouf, followed by a jobs and internship panel. The panel, moderated by Presidential Postdoctoral Associate Eduardo Camps, featured Maxime Bros, Mathematician in the NIST Cryptographic Technology Group; Maalouf; Emma Meno, Research Associate with the Intelligent Systems Division at Virginia Tech National Security Institute; and Virginia Tech Ph.D. student Julia Shapiro. The event provided students with valuable insights into the diverse career opportunities available in these organizations, offering inspiration for their future paths.

- **VT-Swiss Coding Theory and Cryptography Summer School and Collaboration Workshop:**VT-Swiss Coding Theory and Cryptography Summer School and Collaboration Workshop hosted at the Steger Center in Riva San Vitale, Switzerland, was held July 1-5, 2024. There were 64 participants from 20 countries, working across 10 projects and giving 50 presentations. It was a full week of mostly PhD students, postdocs, and early-career faculty in research led by more advanced researchers in the community.

FY25 Node Support Internships

- Triple Point Security Subsidized Internships (33 interns): Triple Point Security brought on 33 new cybersecurity interns as part of our long-standing commitment to the workforce development and regional capacity building in Southwest Virginia. The internship program expanded to its largest cohort yet, providing students from Virginia Tech and Radford with a rigorous 12-week training experience. The technical curriculum focuses on core topics in cybersecurity risk, cloud infrastructure, and DevOps, preparing interns to support real-world technical projects in the fall under the supervision of our full-time consulting team.

- CCI SWVA Internal Internships (2 interns): These internships involved learning program/project management and research administration for a statewide initiative. The internships included event management, website maintenance, and other administrative tasks for the successful implementation of node-wide programs and events.

- Virginia Cyber Range Internships (4 interns): The Virginia Cyber Range infrastructure includes an integrated cybersecurity capture-the-flag competition platform created by our software development team called CloudCTF. Capture-the-flag (CTF) is a competition format that includes challenges across multiple cybersecurity topic areas, such as cryptography, networking, reconnaissance, web, reverse engineering, and others. This grant is to sustain our capability to provide new and interesting CTF challenges by employing student interns who have CTF experience and requisite skills. They have had great success with students in this role.

- Research Internships (6 interns): Dr. Muhammad Gulzar, PI, supported an undergraduate research assistant intern working on a research project entitled "Enhancing the Safety of Users with Disabilities with Inclusive and Transparent Third- Party Web Content." Another PI, Tabitha James, had a student intern work on the question of whether or not they can stimulate a social identity (e.g., an organizational identity), and will the stimulated organizational identity influence the privacy decisions (information disclosure decision) being made. Dr. Yaling Yang, PI, supported four (4) high school students working on her project "Real-time Integrated Misinformation Campaign Alarm and Tracking System in the Age of AI."

- VT Multicultural Academic Opportunities Undergraduate Summer Research Internship Program (6 interns): MAOP provides prospective interns with a diverse selection of mentoring faculty and a description of their research so the student can choose the area of research best suited to their specific interests. This 10-week research program provides motivated undergraduate students across the Nation the opportunity to work with Virginia Tech faculty dedicated to mentoring high-achieving students. The primary goal of this program is to provide students with experiences that cultivate their career goals.

3.2.4 Central Virginia Node

- **CVN Workforce Development Grant FY25:** CVN-funded workforce development programs build on the expertise of higher education institutions that are members of the CVN network, extending opportunities aligned with CCI to students across the commonwealth. The objective is to enhance students' essential skills to enter the cybersecurity workforce once they finish their current studies. We're particularly interested in projects that expose students to experiences in the industry. This grant supports programs that align with CCI's overall mission and CVN's focus areas. CVN awarded three grants, two to VCU and one to VSU, for a total of $150,000.

  In FY25, CVN had over 1,000 applications for CVN-supported internships. 38 interns participated in experiences ranging from short-term internships over the summer with local start-ups and the Federal Communications Commission to long-term internships that ran through the academic year in partnership with the Virginia State Police (Cyber4n6). In addition, UVA hosted an AWS Bootcamp that engaged 60 students. CVN supported Jack Davidson, Ph.D., in FY25. This support allowed Dr Davidson the time and resources to pursue and secure a coalition of Virginia institutions of higher education working in concert as the VA Cyber Navigator Internship Program (VA-CNIP). VA-CNIP includes George Mason University, James Madison University, Norfolk State University, Old Dominion University, University of Virginia, Virginia Commonwealth University, and Virginia Tech. This coalition supports students of the Commonwealth through offering mentorship and internship opportunities. This year, CVN funding supported UVA teams to compete in the International Security Talent Search Competition (ISTS), the Collegiate Penetration Testing Competition (CPTC), Virginia Cyber Fusion, Mid-Atlantic Cyber Defense Competition (MACCDC), and the National Collegiate Cyber Defense Competition (NCCDC). These competitions are briefly described below. The International Security Talent Search (ISTS) competition is held each year at the University of Rochester. ISTS brings together eighteen collegiate teams from across the country for a hands-on, student-built cybersecurity competition to test a wide range of skills. Selected universities send teams of five students, and RIT completes the roster with the winners of our internal red vs. blue competition. Over the course of the competition, teams face a barrage of technical challenges that test their skills in system hardening, incident response, technical writing, and more. The competition is designed to be a fun and educational experience, allowing students to apply their knowledge while also learning from their peers and

industry professionals. The Collegiate Penetration Testing Competition (CPTC) focuses on mimicking the activities performed during a real-world penetration testing engagement conducted by companies, professional services firms, and internal security departments around the world. The Virginia Cyber Fusion Competition and Virginia Cyber Cup Competition are state-wide collegiate competitions hosted by CCI and the Virginia Cyber Range. The UVA team finished in second place in 2025. The Mid-Atlantic Cyber Defense Competition (MACCDC) is the regional qualifier for the National Collegiate Cyber Defense Competition (NCCDC). The UVA team finished first, thereby qualifying to compete in the NCCDC. The team finished in second place.

- **Cyber4n6:** This industry-focused experiential learning opportunity for students bolsters their skillset and resumes, resulting in a highly qualified cyber workforce in the commonwealth. Students work 10 hours per week during the academic year with the esteemed Computer Evidence Recovery Section (CERS) at the Virginia State Police office in Richmond, VA. Serving as a direct pipeline into the real world of digital forensics, students gain hands-on experience that will set them apart in the tech industry.

- **Cypher-Bridge:** In a powerful partnership between the Federal Communications Commission (FCC) Enforcement Bureau (EB) and Virginia Commonwealth University's College of Engineering (VCU-CoE), Project CYPHER (Cybersecurity and Privacy Harnessing Engineering & Research) invites you to be part of an elite fellowship—Project CYPHER-Bridge. Project CYPHER-Bridge is more than a summer program; it's an immersive research experience that empowers you to shape the future of digital security. Dive deep into IoT behavioral forensics and data science and contribute to research with real-world policy implications at the federal level. This is your chance to be part of work that transcends the classroom and directly informs how we secure connected devices and digital infrastructure.

- **CVN Summer Internships:** VCU's Career Services Department worked with local start-ups to secure internship opportunities for CVN students in fields related to cybersecurity, AI, and data. Students from VCU, UVA, and VSU participated in these internships.

- **UVA Summer Internships:** The industry-focused experiential internships supported students applied-learning focused on cybersecurity fundamentals. Some experiences were team-based cyber projects and some were 1:1 internships, but all focused on cybersecurity

- **UVA AWS Bootcamp**. Through a partnership with Amazon Web Services (AWS), UVA facilitated a series of experiential learning programs that educate and engage students in cybersecurity-focused career experiences. In this week-long program, participants gained cloud training that addresses cyber challenges and hands-on activities with visits from Booz Allen Hamilton and the Cybersecurity Infrastructure and Security Agency.

Chapter 4

CCI Innovation

This chapter summarizes the main achievements in FY25 for the CCI innovation mission line, in particular, the results of innovation and commercialization programming.

4.1 Hub-led Programs

4.1.1 Tech Transfer Support Fund

In FY25, the CCI Hub continued the Tech Transfer Support Fund. CCI is offering technology transfer support funding to faculty at primarily undergraduate institutions to facilitate research commercialization efforts. Eligible faculty may apply for grants up to $8,000 to support patent application fees, legal fees, or other professional support. Faculty must enroll in Innovation Commercialization Assistance Program (ICAP) upon grant approval to continue their commercialization efforts.

4.2 Node-led Programs

In addition to the CCI network-wide programs the Hub administered, the CCI Hub again partnered with the NoVA Node to fund our Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT) translational research program, our Academic Support for Cybersecurity Entrepreneurship and Next-Gen Development (ASCEND) program, and Commonwealth Cybersecurity Incubator Accelerator (CCI+A) program, all further described below. The four CCI Nodes also funded several innovation programs.

4.2.1 Northern Virginia Node

In FY25, CCI NoVa Node made investments to expand the number of new cybersecurity solutions in the commercial market by supporting faculty and early-stage companies with wrap-around services to promote the successful development of nascent technologies. In FY25, CCI NoVa Node repeated its support of the highly successful Innovation Commercialization Assistance Program (ICAP) through the continued investment for the cybersecurity accelerator based out of George Mason University's Mason Square Arlington Campus, in the heart of the budding Rosslyn-Ballston Tech Corridor.

- **Innovation Commercialization Assistance Program.** ICAP provides long-term mentorship and advising to early-stage, Virginia-based technology companies, and has assisted more than 1200 companies since the program's inception in January 2018. Cybersecurity-related ventures are one of the main focus areas of the program, with roughly 15 percent of all companies over the past five and a half years having been cyber-focused. In FY24, ICAP, in partnership with George Mason University, began offering access to an NSF I-Corps Lean Startup training program. This program helps participants make the right first steps toward bringing their research to market. Following this course, ICAP Mentors work with clients to provide strategic guidance, connecting them to the right resources at the

appropriate time. ICAP Mentors also assist more advanced startups and later-stage cyber companies by preparing them to join accelerator programs, receive investment, and grow their ventures. During FY25, ICAP engaged with 33 companies that have completed the CCI+A, including the 10 teams from the 2025 cohort. Cybersecurity companies from previous CCI+A cohorts raised $558,000 in capital and created 15 new jobs in FY25. Additionally, one of these companies, AmpSight, was acquired by Vibrint for a confidential, undisclosed amount. This move allowed Vibrint to expand and provide capabilities in cloud engineering, cybersecurity, and artificial intelligence.

- **Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT)**. In 2025, CCI continued support for its Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects amongst CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. The CATAPULT Fund is supporting five (5) new awards in FY25 of $75,000 each. Additionally, CCI is excited to introduce the Academic Support for Cybersecurity Entrepreneurship and Next-Gen Development (ASCEND) Fund for 2025, a mechanism designed to help early-stage companies and startups access and partner with academic subject matter experts to develop and further advance solutions to technical problems they've encountered in industry. The ASCEND Fund is supporting an additional five (5) new awards in FY25 of $75,000. Both funding tracks trigger recipients' participation in the Commonwealth Cyber Incubator + Accelerator (CCI+A). An investment of $500,000 by CCI NoVa Node was supplemented with $300,000 in funding from CCI Hub. CCI+A is an important tool in CCI's Innovation toolbox, providing funding critical to advance the maturity of cyber discoveries during the critical "Valley of Death" phase of commercialization, as defined by the National Science Foundation. During this phase, innovators are preparing for SBIR or CRCF grants to assist in product development and market testing, but are not quite prepared for outside investment. The CATAPULT & ASCEND Funds and the CCI+A Program are helping innovation teams pay for critical resources, personnel, time to test products, and get initial market feedback, integral to obtaining Seed or Angel funding.

  Launched in early 2022 in the new Digital Innovation Pilot facility at George Mason University's Mason Square campus. CCI+A offers: (1) a bootcamp-style program to rapidly move new technologies forward; (2) support for customer discovery efforts; (3) opportunities for cyber startups to engage with potential industry and government partners, as well as broader DMV and commonwealth-based customers; (4) opportunities for customer engagement; (5) opportunities to bring university innovation to industry and government for feedback and collaboration; (6) industry and government collaboration opportunities for cyber faculty on technical work and product testing; (7) opportunities for training students for work in cyber startups; (8) engagement with meaningful student projects; (9) cyber-focused hack-a-thons; (10) cybersecurity-focused workshops, meetings, and collider events with government agencies and industry; and (11) opportunities to engage with seed and venture capital, including the opportunity for exposure to investors and for potential prize money at Mason's annual Accelerate innovation competition. The call for proposals for the CATAPULT and ASCEND Funds were released in January 2025, with proposals due March 10, 2025. Ten (10) new companies and faculty partners were notified of their successful selection for CATAPULT funding in April 2025.

  - *DeepScan* Threat Scanner for On-Device AI; Rui Ning, ODU. As AI becomes pervasive in everyday technology, ensuring the trustworthiness of on-device models is increasingly crucial. While traditional cybersecurity solutions focus on software binaries and network traffic, they cannot reveal whether a neural network itself has been compromised, resulting in significant security gaps, as models may appear normal until triggered to perform harmful actions. DeepScan is an innovative cybersecurity solution that safeguards AI models directly on user devices, running efficiently and locally to protect users' devices in real-time.
  - *RAEMAP: Advancing Secure Real-Time Eye-Tracking for Next-Gen Training and Assessments*; Sampath Jayarathna, ODU. Eye tracking is performed in industry and research across a variety of fields, including education, simulation training, neurocognitive evaluation, human autonomy teaming, and product usability analysis. Advancements in eye-tracking technology have enabled its use on individuals performing day-to-day activities, driving interest in real-time generation

of gaze metrics to analyze how individuals engage with their environment, and examining the relationship between gaze metrics and cognitive activity. Currently, no software in the market exists that can compute advanced gaze metrics in real time from eye tracker data streams. The Real-Time Advanced Eye Movements Analysis Pipeline (RAEMAP) addresses these limitations by providing real-time computation of both positional and advanced gaze metrics.

- *Distortion-free Multi-bit Watermarking for Large Language Models*; Massieh Boroujeny, Mason. Large Language Models (LLMs) can generate remarkably human-like text, which is both a powerful tool and a potential liability. In the wrong hands, LLM-generated content can be misused in ways that harm both individuals and society. A particularly alarming threat is the use of LLMs to mass-produce misinformation and fake news. Because LLM text is often indistinguishable from human-written text, it can be weaponized to sway opinions or perpetuate false narratives at scale. Current LLM watermarking solutions either cause distortion or are computationally inefficient and not scalable. This project addresses these shortcomings, introducing a multi-bit watermarking algorithm for distinguishing human-generated text from AI-generated ones and providing metadata information about the AI-generated text without losing fidelity.
- *Obfuscating Text and Images for Data Loss Prevention*; Mingkui Wei, Mason. Corporate data loss can occur due to various factors, including cyberattacks, insider threats, and web scraping and data mining. While cyberattacks are highly visible and widely recognized, insider threats and web scraping pose even greater risks due to their subtle nature and lack of well-established countermeasures. Unlike cyberattacks – where mature security practices and defense mechanisms exist – insider threats and web scraping take various forms and are harder to detect and prevent, making them an ongoing challenge. This project introduces a series of proprietary technologies to safeguard against data loss caused by insider threats and web scraping, protecting web-based content, including text, images, and documents, while simultaneously ensuring that human users can still view and browse the content normally.
- *Ultra-Sub-Wavelength Polarization Transmitting Embedded Nano-Antenna for Secure and Tamper-Resilient Communication*; Supriyo Bandyopadhyay, VCU, Dong Ha, VT, Fariborz Lohrabi Pour, VT. In classical communication, encoding information in the polarization of an electromagnetic wave offers some advantages, such as polarization-encoded secret sharing. Furthermore, multiple data streams can be sent on the same frequency channel using different polarization states. Polarization of the electromagnetic (EM) state is the preferred method of ferrying information due to the complexity of devices needed to alter polarization. This project introduces a product that allows for polarization-encoded secure information transmission with embedded transmitters and receivers, leveraging novel components of sub- micron dimensions.

FY25 Awardees from ASCEND Fund

- *Distributed Energy Systems (DES) Business Planning through Digital Twin*; Ross Gore, ODU, Taurus nuEnergy. The rapid expansion of Distributed Energy Resources (DER) and Virtual Power Plants (VPPs) has introduced significant challenges in operational efficiency, workforce training, cybersecurity, and regulatory compliance. Supervisors, cybersecurity analysts, and users of DER/VPP systems in these environments lack cognitive control over digital component interactions due to the complexity level. As a result, DER/VPP systems are often poorly understood by those working on the inside and are left vulnerable to exploits like spooking, DDoS attacks, and data integrity breaches from external attackers. Taurus nuEnergy's Digital Twin+ allows operators to anticipate emergent behaviors in control systems, network traffic, and their physical interactions. Additionally, it will enable real-time cybersecurity risk assessment and auto-generate network topology rules, firewall policies, and access controls based on customer requirements and regulations.
- *Securing Computer Code using Dynamically Generated Digital Signatures*; Kun Sun, Mason, CodeLock, Inc. Traditional vulnerability detection methods, rooted in outdated virus protection techniques from the 1990s, struggle to keep pace with the rapid evolution of threats, especially with the rise of generative AI-driven malware. Additionally, open-source software (OSS) is widely

used in both free and proprietary applications, with reports showing that 96% of scanned applications contain OSS, accounting for an average of 57% of their code base. Vulnerabilities in upstream OSS are quickly propagated to downstream applications, and the unreferenced cloning or reuse of OSS makes it difficult for maintainers to track and mitigate security risks. Customers no longer simply need detection – they require an automated mechanism to fix and mitigate vulnerabilities as they arise. While CodeLock's existing solution helps detect unauthorized code changes and known vulnerabilities. This work will integrate automated security patching capabilities into its existing capabilities, introducing a solution capable of addressing both known and previously unknown vulnerabilities in source code.

- *AI=Driven Defensive Cyber through Integrated Zero Trust*; Massimiliano Albanese, Mason, OneTier Corporation. Cyber threats targeting public sector agencies and critical industries have surged in both volume and sophistication, endangering essential services, public trust, and economic growth. The financial and operational impacts underscore the urgent need for next-generation cybersecurity solutions. However, many organizations remain vulnerable due to legacy infrastructure, siloed defenses, and a shortage of skilled cybersecurity professionals. The Zero Trust Command Center (ZTCC) directly addresses these challenges by integrating AI-driven threat detection with a modular Zero Trust framework, delivering proactive and adaptive defense. ZTCC automates security tasks that currently consume hours of analyst time, proactively detecting threats, flagging vulnerabilities, and generating adaptive security responses, in turn allowing human operators to focus on strategic oversight and policy decisions.
- *Combating Crypto Risk*; Foteini Baldimtsi, Mason, FraudOptics; The rapid expansion of the cryptocurrency market has fueled a corresponding rise in illicit activities. Between 2021 and 2023 alone, illicit digital wallets received a staggering $86 billion in cryptocurrency, with illicit crypto activity doubling every 12 months. Traditional blockchain analysis, while useful, is constrained by its focus on on-chain data, leaving a significant gap in understanding and combating financial crimes associated with cryptocurrencies. Existing solutions, primarily based on blockchain analysis, provide valuable insights but are limited to on-chain transactions. This excludes critical off-chain data that offer a more holistic view of cryptocurrency-related risks such as fraud, money laundering, terrorist financing, and ransomware. These gaps hamper the ability of organizations to fully comprehend the complex networks and behaviors of illicit actors in the crypto space, necessitating a more comprehensive approach. Moving forward, FraudOptics aims to address these challenges through a targeted B2B advanced risk intelligence solution.
- *Secure Mesh Communications with Durable Multi-protocol Handover*; Brian Mark, Mason, Kai Zeng, Mason, Critical Shift Corporation. Current solutions to assist military and first responders collect vital data in real-time involve expensive, analog tactical radios or single-protocol digital devices that lack resilient failover capabilities. Critical Shift is addressing these issues with a novel solution that marries integrated hardware-software solutions and secure wireless communications.

4.2.2 Coastal Virginia Node

A key indicator of achieving the goal of growing the cybersecurity business ecosystem in Virginia is the ability to create new cybersecurity businesses from work associated with CCI. CoVA CCI is working with entrepreneurial centers located within our region to support the work of researchers and students who are developing potential business ideas.

- **RAEMAP LLC.** The Real-Time Advanced Eye Movements Analysis Pipeline (RAEMAP) is a software platform for real- time eye-tracking and cognitive state monitoring. By leveraging mobile edge computing, it ensures low-latency analysis of analyst attention and mental fatigue, thereby reducing human error and strengthening cyber defense. RAEMAP is optimized for mission-critical environments, including defense operations, AR/VR training, and human-autonomy teaming. Sampath Jayarathna, Ph.D., Old Dominion University, Computer Research Scientist, Autonomous Integrated Systems Branch, NASA Langley Research Center, Hampton, VA

– **Innovation Spotlight: Jackson Walker**, Christopher Newport University (Class of 2024), BS in Cybersecurity, Computer and Information Systems Security. "It was great to see the range of cybersecurity initiatives the CCI supports through the Project-Based Learning program and how it brings together students, researchers and industry mentors around meaningful, hands-on work like developing web-based CTF challenges, building cloud infrastructure for SOC training labs, exploring wireless vulnerabilities in real-world devices, and examining the intersection of AI security and effective cyber communication" said Jackson Walker, CCI Symposium, April 2025. *Background:* Jackson Walker participated in the CCI Project-Based Learning Program with Microsoft using the Flipper Zero. The Flipper Zero is a small handheld electronic device that can capture and replay many over-the-air signals. It has been used to hack remote controls, garage doors, and other electronic devices. During this program, the selected students worked with their mentor to find ways to leverage the capabilities of the Flipper Zero and to determine if more safeguards are needed to protect the public. After experimenting with the Flipper Zero, including jamming car key fobs and deploying rogue access points, Jackson recognized the need for a unified system to monitor and analyze the wide range of protocols the device can interact with. That insight led to the development of a full-stack Azure telemetry solution for collecting and monitoring wireless IoT lab devices across BLE, Wi-Fi, and Sub-GHz protocols. The system converts raw packet data into structured, queryable insights using IoT Hub, Stream Analytics, Blob Storage, Cosmos DB, and Azure Data Explorer. To improve real-time visibility, he implemented BLE spam detection and integrated live alerts into Azure Sentinel, enabling automated threat monitoring across the lab environment. To complement the telemetry system and give network engineers a new perspective, he developed a custom 3D visualization tool that simulates networks in three-dimensional space and allows real-time observation of device behavior, providing deeper insight into wireless interactions and potential anomalies. He continues to develop this tool, which he calls "NetScry." *Project Summary:* NetScry: Transforming Network Visualization and Security Management. NetScry was born from Jackson's work in CCI programs, tackling a key challenge in cybersecurity and network management: the difficulty of understanding complex network infrastructures and their security postures in real time. *The Problem:* Network engineers and cybersecurity professionals find it hard to visualize their networks comprehensively, which makes it difficult to identify vulnerabilities, ensure policy compliance, and understand data flows within their infrastructure. *The Solution:* NetScry offers a 3D visualization platform that turns abstract network data into an interactive, spatial experience. It captures live network information and maps each device to its actual physical location in 3D space, displaying real-time packet flows as they move between nodes. Users can pause the visualization at any moment to inspect individual devices or packets and access detailed information about protocols, headers, and data contents. Beyond Visualization: The roadmap for NetScry includes a "Network Interpreter" feature that will overlay cybersecurity policies and regulations directly onto the 3D network map. This will allow engineers to immediately see which devices are subject to specific organizational policies, simplifying compliance tracking and security audits. *Market Impact:* By making complex network analysis accessible through any web browser, NetScry democratizes advanced network visualization tools that were previously limited to specialized software. This approach broadens access to the technology for educational institutions, small businesses, and professionals who require powerful network insights without enterprise-level infrastructure. This project demonstrates how academic research can evolve into practical solutions that address real industry needs, transforming theoretical knowledge into accessible technology for both educational and professional markets. Currently, NetScry is being redeveloped as a browser-based tool so it can be used anywhere by anyone.

4.2.3 Southwest Virginia Node

The Southwest Virginia Node funded two programs under the innovation and commercialization mission line. The total investment of Innovation Grants by the Southwest Virginia Node is $250,000. The total investment for other innovation programs by the Southwest Virginia Node is $61,575, for a total FY25 Innovation Investment of $311,575.

- **Program: Ideation to Commercialization**. Innovation: Ideation to Commercialization (IIC) projects should focus on translating the work from the lab to a commercially viable product. The product development process includes idea generation, screening, concept development, product development, and commercialization. The objective of this Call for Proposals (CFP) is to further innovation and product development by funding a project to the subsequent stage(s) in the process. For example, the team may propose funds for 1) market research (concept development) if that is the next stage of the product development, or 2) prototype creation (product development), or 3) other mechanisms to advance commercialization. This call supports business projects related to CCI focus areas, including those that will result in either an operational prototype or further the start- up/product in its development, such that the PI applies for the SBIR/STTR program. The SWVA Node awarded 5 Innovation: Ideation to Commercialization grants. All grants were issued to Virginia Tech for a total of $250,000.
- **FY25 Cyber Innovation Scholars Program:** A group of 34 doctoral candidates, master's students, and postdoctoral researchers attended the Cyber Startup Lab, where they were introduced to processes involved in commercializing cyber technology. The 2025 Cyber Innovation Scholars hail from departments across Virginia Tech, including business information technology, computer science, electrical and computer engineering, and mathematics. The single-day event furthered CCI's mission to cultivate the next generation of the cyber workforce and make Virginia the best place to start a cybersecurity business. Led by Mark Mondry, director of Virginia Tech's LAUNCH and CCI Southwest Virginia's associate director for partnerships and engagement, the workshop combined seven hour-long start-up labs into a half-day marathon, touching on some of the most critical issues to consider before creating a startup. 2025 Cyber Innovation Scholars were also joined by members of the 2024 cohort to participate in a regional innovation event.

4.2.4 Central Virginia Node

This year, CVN supported two faculty innovation projects:

- - Madhur Behl, Ph.D. at UVA, funded through FY25 CVN Innovation and Commercialization funding, is pursuing an SBIR in the fall. This pursuit is a result of Smart City research that has also led to a proposal submission to Toyota Research and a paper submission to IEEE Transactions on Intelligent Transportation Systems. Dr Behl also gave a high-profile keynote address at MARS (Machine learning, Automation, Robotics, and Space), an annual event hosted by Jeff Bezos.
- Nikolaos Sidiropoulos, Ph.D., filed a design patent this year related to interference-resilient antennas. He has met with a VC and veteran entrepreneur and is considering launching a spinout company. He is in the first stage of an STTR and has proposed Phase II.

Chapter 5

Collaborative Partnerships and Projects

5.1 Partnerships

Industry/University Cooperative Research Centers

In the last fiscal year, we launched a new IUCRC, co-funded by NSF and industry: the WISPER IUCRC focuses on the development of secure 6G technologies. In these highly competitive grants, NSF provides core funding for the administration and management of the center, and industry has the leading role in funding and selecting research projects to be conducted. WISPER currently has 13 industry members and brings in approximately $1 million in funding every year; the center is led by the CCI Executive Director and involves Virginia Tech, Mason, and the University of Arizona.

This year, we also joined another IUCRC, Cyber SMART, with a focus on cybersecurity solutions; Dr. Gretchen Matthews, CCI Southwest Virginia Node Director, also serves as site director at Virginia Tech for Cyber SMART. Another large-scale industry collaboration of note is the ACCoRD project, funded by NTIA and led by AT&T and Verizon. Key portions of this $42 million research and testing project are conducted in the CCI xG testbed.

Approximately 30% of the research funding that CCI researchers attract comes from the private sector and partnerships, such as the ones described here.

Department of Defense Industry-specific Training

In FY25, VCU received the final disbursement of a $17.8 million project funded by the U.S. Department of Defense and supporting a unique industry-academia partnership for industry-specific training and hands-on research for graduate and undergraduate students. This project, the Convergence Lab Initiative, was launched by the CCI Central Virginia Node Director, Erdem Topsakal.

O-RAN Alliance

In Fiscal Year 2021 (FY21), CCI joined the O-RAN Alliance, whose objective is to transform the radio access networks industry towards open, intelligent, virtualized, and fully interoperable Radio Access Network (RAN). The expectation is that O-RAN standards will enable a more competitive and vibrant RAN supplier ecosystem with faster innovation, and that O-RAN-based mobile networks will improve the efficiency of mobile network deployments and operations.

Using our NextG testbed, CCI is doing world-leading work in the integration of an open source 5G implementation, srsRAN, with the O-RAN architecture.

Next G Alliance

The Next G Alliance is an initiative to advance North American mobile technology leadership over the next decade through private sector-led efforts. With a strong emphasis on technology commercialization, the work encompasses the full lifecycle of research and development, manufacturing, standardization, and market readiness.

CCI is a contributing member of the Next G Alliance, with our researchers participating in each of the working groups of the Alliance. This provides a path to impact the emerging vision for 6G and to translate our researchers' work into commercially adopted solutions.

5.2 Correlated Economic Outcomes

In FY25, CCI commissioned RTI International to conduct the third economic impact study for fiscal years 2024 and 2025. In FY 2024 and FY 2025, CCI reported continued growth in many of its key metrics for impact. Below is a list of new highs recorded in FY24 or FY25 for some CCI metrics.

- $127.8 million in external R&D funds attracted (FY24)
- $5.2 million in venture capital raised by startups (FY24)
- 13 jobs reported as directly created by startups (FY24)
- 11 new filings for intellectual property (FY24)
- 1,118 undergraduate students served (FY24)
- 15 filings for intellectual property (FY25)
- 15 jobs directly created by startups (FY25)
- 534 students participating in workforce and experiential learning programming (FY25)

5.2.1 Economic Impact Study Modeling

RTI International used IMPLAN, an input-output model, to render the state economy and capture transaction and spending flows across industries and through employee spending. IMPLAN can estimate the total impact of industry activity when either output (spending) or employment is known for a specific industry or economic event.

- **Jobs:** IMPLAN's measurement of jobs consists of all full-time, part-time, and temporary positions. Jobs are reported as an annual average. Direct jobs are those created with CCI funding, such as program administrators, faculty, and program researchers. Indirect jobs are those supported by CCI program spending among local businesses. Induced jobs are supported by CCI employees and employees at businesses with CCI contracts, spending their wages in the local economy.
- **Labor Income:** Labor income is a component of value added and represents multiple forms of employee compensation, including wages and benefits, and proprietor income, which consists of income from self-employed individuals and independent business owners. Labor income indicates how much additional personal income is created by CCI activities.
- **Value Added and Output:** Value added and output are both ways to measure the size of specific industries and the economy as a whole. Value added provides an indicator of the labor, capital, and tax income generated from production activities. Value added is also referred to as "gross domestic product (GDP).
- **State and Local Tax Revenue:** State and local tax revenues are the sum of tax revenue that will be generated at the sub-county, county, and state levels. These taxes include items such as state income taxes, corporate business taxes, sales taxes, and special district fees.

5.2.2 Economic Impacts of CCI Activities: FY24 and FY25

In FY24, CCI's activities supported a total of **1,181 jobs**, earning an estimated **$94 million** in labor income and **$136.5 million** in economic activity, as seen in Figure 5.1. These activities generated an estimated **$8.1 million** in combined state and local government revenues, including an estimated **$5.6 million** in Commonwealth of Virginia revenues.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Tax Revenues ($M)
Direct	566	$53.6	$65.8	$135.0	$2.8
Indirect	351	$25.2	$39.8	$70.1	$2.4
Induced	264	$15.1	$30.8	$48.3	$2.9
Total	1,181	$94.0	$136.5	$253.4	$8.1

Source: IMPLAN, RTI analysis of FY 2024 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.1: Economic Activity Supported by CCI in Virginia in FY25.

In FY25, CCI's activities supported a total of **960 jobs**, earning an estimated **$79 million** in labor income and **$114.3 million** in economic activity, as seen in Figure 5.2. These activities generated an estimated **$7.8 million** in combined state and local government revenues, including an estimated **$4.6 million** in Commonwealth of Virginia revenues.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Tax Revenues ($M)
Direct	469	$45.4	$55.8	$111.3	$2.7
Indirect	277	$20.8	$32.8	$56.9	$2.3
Induced	214	$12.7	$25.7	$39.9	$2.9
Total	960	$78.8	$114.3	$208.0	$7.8

Source: IMPLAN, RTI analysis of FY 2025 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.2: Economic Activity Supported by CCI in Virginia in FY25.

5.2.3 Region-by-Region Breakdowns for FY24 and FY25

In each of the four regions served by the CCI nodes and Hub, CCI activities contributed to jobs, labor income, output, and state and local government revenues, see Figures 5-3 through 5-10. The 1,181 jobs supported by CCI are broken out in the following section, with the four nodes' contributions to their regions. Regional activities funded by the Hub are allocated to the region where they took place, and direct Hub activities in Northern Virginia are allocated to Northern Virginia.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	57	$5.3	$6.3	$13.5	$0.3
Indirect	38	$3.1	$4.9	$8.2	$0.3
Induced	33	$2.0	$4.0	$6.2	$0.4
Total	127	$10.4	$15.2	$27.9	$1.0

Source: IMPLAN, RTI analysis of FY 2024 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.3: Economic Activity Supported by CCI in Central Virginia in FY24.

	Jobs	Labor Income ($M)	Value Add ($M)	Output	State and Local Government Revenues ($M)
Direct	121	$11.9	$14.4	$30.3	$0.5
Indirect	85	$5.5	$9.0	$16.1	$0.4
Induced	68	$3.5	$7.3	$11.8	$0.4
Total	274	$20.9	$30.7	$58.2	$1.3

Source: IMPLAN, RTI analysis of FY 2024 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.4: Economic Activity Supported by CCI in Coastal Virginia in FY24.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	222	$24.9	$30.9	$53.8	$1.3
Indirect	104	$9.4	$15.0	$24.1	$0.8
Induced	92	$6.2	$12.2	$18.3	$1.2
Total	418	$40.4	$58.1	$96.3	$3.3

Source: IMPLAN, RTI analysis of FY 2024 CCI spending data, includes hub activities that take place in the Northern Virginia region.
Note: Columns may not sum due to rounding.

Figure 5.5: Economic Activity Supported by CCI in Northern Virginia in FY24.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	166	$11.6	$14.2	$37.3	$0.7
Indirect	124	$7.3	$11.0	$21.7	$0.8
Induced	71	$3.5	$7.4	$12.1	$0.8
Total	361	$22.4	$32.6	$71.1	$2.3

Source: IMPLAN, RTI analysis of FY 2024 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.6: Economic Activity Supported by CCI in Southwest Virginia in FY24.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	62	$5.8	$7.0	$14.9	$0.4
Indirect	42	$3.4	$5.4	$9.0	$0.4
Induced	36	$2.2	$4.4	$6.8	$0.5
Total	140	$11.4	$16.7	$30.8	$1.2

Source: IMPLAN, RTI analysis of FY 2025 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.7: Economic Activity Supported by CCI in Central Virginia in FY25.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	61	$5.9	$7.1	$14.9	$0.4
Indirect	42	$2.7	$4.4	$7.9	$0.3
Induced	33	$1.7	$3.6	$5.8	$0.4
Total	137	$10.3	$15.1	$28.6	$1.1

Source: IMPLAN, RTI analysis of FY 2025 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.8: Economic Activity Supported by CCI in Coastal Virginia in FY25.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	227	$25.5	$31.6	$55.1	$1.4
Indirect	106	$9.6	$15.4	$24.8	$0.9
Induced	94	$6.3	$12.8	$18.8	$1.3
Total	427	$41.4	$59.4	$98.7	$3.6

Source: IMPLAN, RTI analysis of FY 2025 CCI spending data. Includes hub activities that take place in the Northern Virginia region.
Note: Columns may not sum due to rounding.

Figure 5.9: Economic Activity Supported by CCI in Northern Virginia in FY25.

	Jobs	Labor Income ($M)	Value Add ($M)	Output ($M)	State and Local Government Revenues ($M)
Direct	119	$8.2	$10.1	$26.3	$0.6
Indirect	87	$5.1	$7.7	$15.2	$0.6
Induced	50	$2.5	$5.2	$8.5	$0.7
Total	256	$15.8	$23.0	$49.9	$1.9

Source: IMPLAN, RTI analysis of FY 2025 CCI spending data
Note: Columns may not sum due to rounding.

Figure 5.10: Economic Activity Supported by CCI in Southwest Virginia in FY25.

Chapter 6

Financial Report

6.1 CCI Hub

The budget and expenditures for the CCI Hub in FY25 are in Appendix 4.

CCI continued to focus on its three mission lines of research, innovation, and workforce development in FY25. The CCI xG testbed is fully operational, with researchers, students, and industry partners from across the state using it for experiments and research. In FY25, CCI focused on scaling up successful workforce development programs to state-wide participation. These programs continue to show positive results and remain popular. Additionally, CCI will continue to improve upon and share the positive results from the RTI Economic Impact Study for Fiscal Years 2024 and 2025.

Operations continued to support the CCI mission and the research, workforce development, and innovation communities across the state. CCI hosted the 4th annual CCI Symposium in Richmond, VA, and continues to host international delegations, as well as industry and government partners at the VTRC-A, to foster collaboration and continue to expand the cybersecurity ecosystem in Virginia.

Communications and marketing played a major role in advertising, promoting, covering, and branding several CCI-sponsored, co-sponsored, or attended events in FY25. CCI continued to utilize social media platforms and expand our social media footprint to promote CCI events, researchers, and highlight positive impacts across the state in cybersecurity research, workforce development, and innovation. In FY25, several of CCI's social media pages/platforms showed significant increases in hits, views, and likes.

The CCI Hub continued to sponsor Experiential Learning programs, entrepreneurial incubators, and Cyber Fusion 2025. The CCI Hub continued to sponsor and lead several Project-Based Learning programs for Virginia students working for industry partner companies. These programs are very popular and have received positive feedback from both industry partners and students. CCI Hub continued to co-sponsor the CATAPULT and CCI+A innovation programs at the Northern Virginia node.

In FY25, the CCI Hub sponsored the AI for Cybersecurity and Cybersecurity for AI Research Program. This is the CCI Hub's annual state-wide cybersecurity research program to foster collaboration among researchers and provide the initial research results for future large-scale research proposals. This year, the CCI Hub awarded nine grants, and the regional Nodes awarded an additional nine grants under the program. CCI researchers from across the commonwealth continued to attract external funding by submitting high-quality and collaborative proposals that will produce high-impact results and continue to move Virginia to a global leader in cutting-edge cyber innovation and research.

6.2 CCI Nodes

In FY25, the CCI Regional Nodes developed spend plans that supported Node objectives, initiatives, and programs that were aligned with their cybersecurity focus areas and the expertise of their research faculty. The Nodes apportioned their funds into three categories: Operations, Research, and Innovation/Workforce Development. Although the categories are the same and all focused on the cybersecurity field, each Node has the flexibility to plan and execute funds so as to best meet the needs of their region and reinforce the cybersecurity research focus of their region's universities and verticals. In FY25, the Nodes continued to support collaboration across the CCI network of university researchers and students by sponsoring Node-funded and administered collaborative research programs. Additionally, the Regional Node's funded and hosted events, workshops, and initiatives within its region.

6.2.1 Coastal Virginia Node

The budget and expenditures for the CoVA Node in FY25 are in Appendix 4.

The Coastal Virginia Center for Cyber Innovation, as part of the Commonwealth Cybersecurity Initiative, acts as the hub of southeastern Virginia for research, innovation, and the commercialization of next-generation cybersecurity technologies, especially in the fields of Cyber Physical Systems Security and Artificial Intelligence within the maritime, defense, and transportation sectors.

Research Funding: Funds for research support have been allocated to three key areas: ongoing support for research scientists, funding for cybersecurity research, and improvements to the Coastal Virginia Shared Academic and Research Environment. For ongoing funding of research scientists, resources have supported 12 faculty members hired at William and Mary, the Old Dominion University School of Cybersecurity, and the Virginia Modeling, Analysis, and Simulation Center. Additionally, these funds will sustain an IT Engineer responsible for managing research projects related to COVA SHARE. Lastly, funds continue to finance various cybersecurity research projects.

Workforce Development and Innovation Funding: Resources allocated to foster regional innovation and build the talent pipeline have been used to promote experiential learning, support undergraduate research, encourage student-led innovation programs, facilitate cybersecurity internships, and drive commercialization efforts. These funds also provide ongoing support for the Coastal Virginia Cybersecurity Student Association and their annual conference/CTF. The undergraduate research program connects students and faculty across the node on cybersecurity initiatives, while the Innovate Cyber Challenge brings together students from across the commonwealth to develop solutions for cybersecurity challenges.

Operations Costs: The central operations team comprises a chief administrative officer/project manager and includes stipends for additional leadership team members. Operational funds cover program administration, research activities, innovation programs, and workforce development initiatives. These funds are also used to organize meetings, travel, and activities that foster community among members of the Coastal Virginia Center for Cyber Innovation.

6.2.2 Central Virginia Node

The budget and expenditures for the CVN in FY25 are in Appendix 4.

In FY25, CVN continued to use funds to support successful endeavors. Support continued for the testbeds that are available for use by the CCI network and will continue to foster successful startups. In addition, CVN expanded the development of regional partnerships and strengthened the internship program.

Operations funds supported regional staff, a CVN annual meeting, regional partnerships, and general operating expenses.

CVN funds continued to fund several testbeds that are integral to fostering collaboration across the region and the state. In addition, CVN continued to fund a node-wide research call that required collaboration as well as supporting research faculty.

Regional workforce development and commercialization projects were also supported with these funds. The remaining funds were split between VCU and UVA to finance internal calls for commercialization and internships.

6.2.3 Northern Virginia Node

The budget and expenditures for the NoVA Node in FY25 are in Appendix 4.

During FY25, CCI NoVa Node has made major investments in cybersecurity workforce development, attacking the challenge from every potential entry point and through novel modes of training and partnership. NoVa Node also made significant investments in the development of the cybersecurity innovation ecosystem through the establishment of the CATAPULT and ASCEND funds and the CCI+A cybersecurity accelerator to support cybersecurity startups with seed funds and wrap-around services to ensure their success and anchor them in the commonwealth. The NoVa Node's research investments resulted in a mature R&D effort now in direct support of the innovation ecosystem, and serving as a major attractant of external funding to bolster the commonwealth's Cybersecurity research enterprise.

As a portfolio, the Nova Node has specifically developed a sphere of investments that are intertwined. Workforce efforts are in direct support of research and the success of entrepreneurship. Research and development efforts are deliberately and directly embedded in the expansion of the cybersecurity innovation ecosystem. This cohesive framework and record of impact enable CCI NoVa Node to enter FY26 with the ability to scale its success and impact.

CCI Investments in the NoVa Node's operations included support for the full-time project manager who provides day-to-day oversight of CCI NoVa Node programs and partnerships, a portion of the CCI NoVa Node Director's time, as well as additional expenditures relating to the administration of CCI NoVa Node.

In FY25, CCI NoVa Node engaged in recruiting and supporting faculty to the commonwealth. The Mason Living Innovation Laboratory infrastructure and faculty enterprise have significantly matured and are prepared for expansion. We anticipate that the recruitment of new faculty expertise to Virginia and each of the research universities will enable expansion of Northern Virginia's success in competing for new, externally sponsored research funding, including Federal dollars. In FY25, CCI NoVa Node earmarked funding to support the recruitment of an additional faculty member focusing on the areas of Artificial Intelligence (AI) and cybersecurity. Additionally, NoVa Node supported additional research proposals, focusing on the Node's cybersecurity priority areas of impact: national defense, infrastructure, transportation, electric/power distribution, manufacturing sectors, and resilience of cyber systems to human behavior. NoVa Node continued to develop industry and government partners to collaborate and support in material ways, the NoVa Node research portfolio.

In FY25, the CCI NoVa Node continued to make significant investments in cybersecurity-related experiential learning opportunities for high school students, college/university students, and those seeking to upskill into cybersecurity positions in industry and government. These opportunities enabled students to apply classroom knowledge to real-world challenges and bridge the "experience" divide. These investments will grow the pipeline of cybersecurity career-ready talent. In addition, the NoVa Node continued to support each of its program participants to complete clearance preparedness programs to expand the number of students across the NoVa Node who are prepared to enter and complete the security clearance process. Investments were made to upskill non-degree-seeking candidates, with special emphasis on career changers and those without prior cybersecurity training, in order to grow the pipeline. NoVa Node also scaled up its undergraduate internships to prepare our students for work in established or emerging companies working at the leading edge of R&D. CCI NoVa Node continued to build and expand the cybersecurity innovation and entrepreneur ecosystem in Northern Virginia

and across the commonwealth. In FY25, NoVa Node continued its investment in Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects among CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. We also introduced the Academic Support for Cybersecurity Entrepreneurship and Next-Gen Development, a new mechanism designed to help early-stage companies and startups access and partner with academic subject matter experts to develop and further advance solutions to technical problems they've encountered in industry. A key part of the demonstrated success of CATAPULT and the anticipated success of ASCEND has been investment in CCI+A. Our cybersecurity accelerator launched in FY22, providing seed support for 16 new cybersecurity start-ups over the last two years, and the wrap-around services to ensure their successful growth in the commonwealth. In FY25, CCI+A added an additional cohort of new companies. In both the areas of workforce development and innovation and entrepreneurship, CCI NoVa Node is committed to expanding opportunities in the field by actively engaging in both traditional and nontraditional settings to attract increasingly diverse applicant pools for our many programs.

6.2.4 Southwest Virginia Node

The budget and expenditures for the SWVA Node in FY25 are in Appendix 4.

The Commonwealth Cyber Initiative in Southwest Virginia (CCI SWVA) advances Virginia as a global leader in secure cyberphysical systems by promoting cybersecurity research, innovation, and talent development in Southwest Virginia. CCI SWVA partners with researchers who provide technical excellence in wireless communications, emerging technologies, and cybersecurity with unique and expansive capabilities in the application domains such as transportation, power systems, manufacturing, and agriculture, to discover, demonstrate, and commercialize technological solutions that will enable the next industrial revolution.

CCI SWVA supported its programmatic efforts with personnel, including its Program Manager and the SWVA Node Director. Other operational costs include travel and infrastructure expenses.

CCI SWVA supported major research initiatives that built upon prior investments. CCI SWVA continued to fund major research areas, including security of data, communications, power and energy, transportation, and cyberbiosecurity, resulting in programs in quantum communication, artificial Intelligence assurance, 5G/next-G, wireless security, cryptography, wireless communications and security, system and software security, autonomous vehicle safety, and 5G power grid. CCI SWVA also supported post-doctoral associates and the professional development costs for graduate research assistants.

CCI SWVA continued the Regional Innovation thrust by providing funding for an Innovation call for proposals and support of the SWVA innovation community. Talent Pipeline programs included the CCI SWVA Internship Program, designed to incorporate all partner institutions and engage SWVA companies and start-ups. Securitas, a cybersecurity-focused living learning community at Virginia Tech, was supported with funding for the program director and provided programming support with researcher presentations and programs.

6.3 Geographic distribution of the awards from funds contained in HB30

The below Figure 6.1 shows the distribution of awards from funds in HB30.

Node	Number of Awards	Grant Total
Central Virginia	5	$2,910,000
Coastal Virginia	6	$3,050,000
Northern Virginia	3	$2,800,000
Southwest Virginia	5	$2,940,000
Total	**19**	**11,700,000**

Figure 6.1: Geographic distribution of awards from appropriated funds.

Chapter 7

Looking Ahead: FY26

In FY25, we continued to invest in research, innovation, and workforce development programs launched by the CCI Hub and by each of the regional Nodes. Our biannual economic impact study revealed CCI's impressive impact on cybersecurity jobs, engagement with companies and the innovation ecosystem, and active participation by students throughout the network. Most of this report thus far has been devoted to describing the main accomplishments of the CCI network in FY25. In this chapter, we outline the main activities and programs planned for FY26.

Focus area: Critical Infrastructure Cybersecurity

In FY26, we are focusing on building research and workforce capacity in the area of critical infrastructure cybersecurity. This will be the topic of our largest internal call for research proposals, with the objective of building multi-university, transdisciplinary teams with expertise on securing critical infrastructure. The selected teams will use these seed grants to increase their competitiveness in large-scale research grants and contracts from federal agencies and the private sector.

Presidential Policy Directive 21 defines critical infrastructure sectors as: Chemical; Commercial Facilities (e.g., NFL stadiums); Communications; Critical Manufacturing; Dams; Defense Industrial Base, including research universities doing Department of Defense (DoD) research; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Services and Facilities, including local and state government; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water and Wastewater Systems.

Over 80 percent of the United States' critical infrastructure is privately owned and operated. In rural areas, it is common for small cooperatives to provide critical infrastructure services such as electricity distribution. These enterprises rarely have the capacity to staff a security operations center 24/7, evaluate cybersecurity posture, evaluate cybersecurity products, and so on. At the other end of the spectrum, large municipalities such as Fairfax County may have the resources to staff a large cyber fusion center but are also the target of well-funded nation-state actors and criminal gangs.

We will build research capacity in the commonwealth on topics such as:

- AI-informed cybersecurity operations for small and medium-sized critical infrastructure providers.
- Broad, generally applicable horizontal solutions that protect most critical infrastructure sectors.
- Tailored, vertical solutions that protect specific critical infrastructure segments because of the specialized nature of the sector or leverage or address unique characteristics of a sector, such as limited, intermittent connectivity, 30-year equipment lifetimes, legacy installed base, or public policies that inhibit the deployment of modern cybersecurity solutions.

Seed grants to CCI teams will have the following as objectives:

- To produce seminal contributions to critical infrastructure cybersecurity, targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources.
- To foster interdisciplinary collaboration to produce high-quality research with strong domain knowledge, resulting in a high likelihood of future extramural funding.
- To produce research contributions that translate into benefits to Virginia companies.
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) in critical infrastructure cybersecurity.

Strengthening the Cyber Startup Ecosystem

In FY25, we updated our CCI+A incubator and accelerator program to create a specific track to pair up innovators in CCI with cyberstartups in Virginia. We are starting to closely track the impact of CCI innovation, workforce development, and research programs on the startup ecosystem.

This year, we plan to continue to increase our engagements with startups in joint research proposals, to create experiential learning opportunities, and as a vehicle to translate ideas that originated in CCI universities into commercialization.

AI for Cybersecurity and Cybersecurity for AI

Our largest investment area in FY25 was AI for cybersecurity and cybersecurity for AI, providing $1.6 million in seed grants for multi-university teams to build capacity in this important area. We are starting to see the results of this investment more quickly than we anticipated, with a faculty member from UVA receiving a $900K grant from NSF as a result of initial investigations conducted with CCI support.

AI and cybersecurity remain tightly integrated: cybersecurity solutions, from biometrics to intrusion detection, invariably incorporate AI; and all uses of AI must face issues of privacy, data management, and security. In FY26, we will continue to invest in this topic, expanding our focus to include policy issues for secure and trustworthy AI.

Continuous Improvement and Expansion of our Workforce Development Programs

CCI currently runs a wide variety of experiential learning programs, with a focus on providing students with opportunities to work directly with their future employers, through internships, traineeships, project-based learning, and cyber clinics programs. In FY26, we will continue to expand these programs through additional partnerships with Virginia companies of all sizes and state and federal agencies.

Every spring, since FY21, we have been running a solicitation for experiential learning programs to be designed and run by faculty in any of the CCI institutions. This call for proposals has yielded extremely productive partnerships with a range of cyber startups and agencies like the Virginia State Police (for an internship program on data forensics) and the Virginia Department of Elections (for an internship program on election security).

In FY26, we will again run this internal call for proposals, with updated requirements to ensure that students receive valuable workforce experience and increase their job opportunities once they graduate. The most significant change to the requirements will be the level of expected participation from an industry partner. Past projects have featured industry participation in a wide range, from hiring students to providing real-world challenges. In the FY26 iteration, successful proposals must ensure that students work directly with/for the industry partner to maximize their workforce experience.

Partnerships across the Commonwealth

We are starting to work closely with Virginia Works, in the Virginia Department of Workforce Development and Advancement. In FY25, we had a series of discussions with Virginia Works staff, which resulted in agreement on a set of workforce development metrics to be reported by CCI, including the number of participants, retention metrics, and cost per participant. We have been collecting these metrics for CCI's workforce development programs and will start reporting consolidated numbers for FY25.

We continue to interact closely with Virginia Economic Development Partnership (VEDP), showcasing the commonwealth's unique strengths in academia-industry-government partnerships in cybersecurity. We have recently partnered with VEDP on a proposal to RSAC, the leading cybersecurity conference in the world. If the proposal is accepted, the next RSAC, in March 2026, will feature a panel moderated by VEDP and counting on three CCI faculty members to showcase the translational research in cybersecurity taking place in Virginia.

We also continue to engage with local and regional economic development initiatives and groups. In FY25, Dr. Gretchen Matthews, Director of the Southwest Virginia Node of CCI, was named STEM Educator of the Year by the Roanoke Blacksburg Technology Council. In FY26, the CCI leadership is contributing to an initiative to promote the Richmond/Hampton Roads area as an advanced digital technology corridor. And CCI's cyber clinics program continues to grow, with a focus on providing cybersecurity services to the local communities across the commonwealth.

Global Collaborations

There is consensus that international collaboration is critical for cybersecurity, as threats are not confined to national boundaries and sophisticated cyberattacks often require coordinated response and shared intelligence. The NATO Cooperative Cyber Defense Centre of Excellence, for example, has extensively studied and mapped out collaboration in cybersecurity among NATO countries.

CCI continues to establish cooperative research with institutions in Europe and Asia and exchange best practices in talent development with countries that face similar workforce challenges. These activities will continue to accelerate in FY26, building on our recent success in obtaining research funding for collaborations with Finland, Ireland, the UK, and Japan.

Appendices

Appendix 1: CCI Extramural Funding for FY25

Appendix 2: CCI AI for Cybersecurity / Cybersecurity for AI Research Grants FY25

Appendix 3: Node Research Grants FY25

Appendix 4: FY25 Financial Reports

Appendix 1: CCI Extramural Funding for FY25

CCI Hub

Project Title	Institution	Funding Amount	Funding Agency
Accenture Agriculture and Cybersecurity Support Fund	Virginia Tech	$75,000	Accenture
IUCRC Virginia Tech: Center for Cyber Science, Management Applications, Regulation, and Training	Virginia Tech	$50,000	NSF
Washington CORE Projects 2025	Virginia Tech	$84,000	Washington CORE
Establishing Best Practices for Socialization of New Technologies for Effective Integration Post-Acquisition	Virginia Tech	$45,600	Stevens Institute of Technology
Recovery, Reconstruction, and Modernization of Ukraine: Cybersecurity and Supply Chain	Virginia Tech	$1,500	Washington CORE
IUCRC Phase I Virginia Tech: Center for Wireless Innovation towards Secure, Pervasive, Efficient, and Resilient Next G Networks (WISPER)	Virginia Tech	$375,000	NSF
U.S.-Ireland R&D Partnership: NeTS: Small: Fungibility in Mobile Networks for Resilient 6G	Virginia Tech	$248,800	NSF
IUCRC Phase I George Mason: Center for Wireless Innovation towards Secure, Pervasive, Efficient, and Resilient Next G Networks (WISPER)	Virginia Tech	$50,000	IUCRC/Mason
Collaborative Research: CIRC: Planning-C: O-Milli-RAN – An O-RAN-compliant, Softwarized mmWave Radio Stack with Flexible PHY and MAC	Virginia Tech	$30,000	NSF
Byzantine Resilient Federated Learning in Sporadically Connected Wireless Networks	Virginia Tech	$1,500,000	ONR

Project Title	Institution	Funding Amount	Funding Agency
U.S.-Ireland R&D Partnership: NeTS: Small: Fungibility in Mobile Networks for Resilient 6G	Virginia Tech	$552,000	NSF
Trustworthy Generative AI for Secure System Operation	Virginia Tech	$75,000	NSF
Policy study on Trustable technology for Cyber Physical System	Virginia Tech	$58,000	NSF
Recovery, Reconstruction, and Modernization of Ukraine; Cybersecurity and Supply Chain	Virginia Tech	$10,000	Washington CORE
Sustainable Energy-Efficient Digital Infrastructure	Virginia Tech	$5,000	Washington CORE
Total		**$3,159,900**	

Central Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
Modeling and Predicting Causal Effects on Complex Networks	University of Virginia	$400,000	Office of Naval Research
Implementation and Evaluation of Human-in-the-Loop	University of Virginia	$100,000	US DOT / Morgan State University
VA-CNIP: A Coalition for the Virginia Cyber Navigator Internship	University of Virginia	$2,878,985	NSA
Magnaforma	Virginia Commonwealth University	$20,000	National Endowment for the Arts
Leveraging Scholarships and Vertically Integrated Projects to Increase Transfer Undergraduates Engagement, Capacity, and Continuity in Computer Science	Virginia Commonwealth University	$1,997,717	National Science Foundation
Enhancing Multidisciplinary STEM Undergraduate Education through Living Labs	Virginia Commonwealth University	$750,000	National Science Foundation
Electromagnetic Side-channel Monitoring for Detecting Control Logic Attacks in Industrial Control Systems	Virginia Commonwealth University	$250,000	National Nuclear Security Administration
PLC Forensic Toolset for Industrial Control Systems", Department of Homeland Security	Virginia Commonwealth University	$450,000	Department of Homeland Security
Convergence Lab Initiative (CLI)	Virginia Commonwealth University	$2,600,000	Department of Defense
Total		**$9,446,162**	

Coastal Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
Hampton Roads Regional Apprenticeship Hub	ODU	$1,200,000	HRWC
CyberCorps SFS Supplemental Funding	ODU	$75,000	NSF
Collaborative Research: SHF: Medium: End-to-End Resilience in Autonomous Driving Systems: Strategic Vulnerability Assessment and Mitigation	WM	$926,737	NSF
Advancing Health Equity: Integrating LLM Technology into Homeless Telehealth Services for Chronic Disease Education	ODU	$150,000	NSF
DoD Cyber Scholarship Program	ODU	$193,751	NSA
The 3D Cybersecurity Pipeline: Bridging Schools, Higher Education, and Industry	ODU	$200,000	NIST/NICE
Developing AI in Cybersecurity Competency Through Competitions	ODU	$349,606	NSA
Student Training in Quantum Computing	WM	$10,000	Ion Q
5G RDT&E Testbed for Radar Co-existence and Non-Kinetic Effects	ODU	$4,886,415	HII
WRT-1085: TRUSTED ARTIFICIAL INTELLIGENCE (AI) SYSTEMS ENGINEERING (SE) CHALLENGE	ODU	$21,000	SERC
AI Powered UAS Maritime Operations	ODU	$25,000	ODU
Collaborative Research: PACSP TOOLS: EPICS: Explainable AI Driven Individual Photo-Identification and Tracking for Cost-effective Conservation Study	WM	$269,740	NSF
CRII: III: Pursuing Interpretability in Utilitarian Online Learning Models	WM	$175,000	NSF

Project Title	Institution	Funding Amount	Funding Agency
Travel: NSF Student Travel Support for the 2024 IEEE International Conference on Data Mining (IEEE ICDM 2024)	WM	$25,000	NSF
AI-powered Underwater Optical Survey for Benthic Biomass and Sediments Assessment	WM	$30,000	NSF (IUCRC)
CRII: III: Dynamic Prompting and Pruning for Measuring and Controlling Memorization in Text-Attributed Graphs	WM	$174,983	NSF
Dynamic spectrum management (DMS) in Future G	ODU	$2,168,334	NSWC
Center of Excellence in AI/ML (5h year)	ODU	$350,000	DoD
HRCF Re-Direct	ODU	$350,000	ODU IRAD
Marketing Cyber Bridge Project	ODU	$45,000	Northeastern University
SFS Supplemental	ODU	$429,359	ODU
Total		**$11,786,185**	

Northern Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
2024-2025 George Mason University Cybersecurity Scholarship Program	Mason	$87,833	DoD
Privacy Preserving Transactions with Accountability Extensions	Mason	$108,782	NSF
ISAC Strategy Summit 2025	Mason	$256,146	ARFL
ISAC Strategy Summit 2025	Mason	$32,465	ARFL
HERA: Hypothesis Evaluation and Reasoning Assistant	Mason	$58,000	ARFL
Synthesizing Temporal Logic and Human Performance Models for Deception Mitigation	Mason	$500,000	ONR
Machine Learning for Space Situation Awareness	Mason	$60,000	ARFL
Innovating Volumetric Video Streaming with Motion Forecasting, Intelligent Upsampling, and QoE Modeling	Mason	$100,377	NSF
Network and Systems Challenges in Immersive Computing	Mason	$99,999	NSF
Scaling up Multi-user Immersive Content Delivery over mmWave	Mason	$180,000	NSF

Project Title	Lead Institution	Funding Amount	Funding Agency
Translation Potential of Next Generation Telepresence Enriched by Immersive Technologies	Mason	$50,000	NSF
Efficient and Scalable Deployment Automation for Quantum-centric Computing	Mason	$641,778	NSF
MACH-Q: Modular and Error-Aware Software Stack for Heterogeneous Quantum Computing Ecosystems	Mason	$40,000	DoE
Engaging Marginalized Groups to Improve Technological Equity	Mason	$439,380	NSF
Encrypted Systems with Fine-Grained Leakage	Mason	$367,867	NSF
Targeted Microarchitectural Attacks and Defenses in Cloud Infrastructure	Mason	$120,000	NSF
Approximate Computing for Machine Learning Security: Foundations and Accelerator Design	Mason	$101,135	NSF
SAFETI: Strategic Analysis for Fine-granular Injury and Fatality PrEvenTion Insight	Mason	$132,000	VDOLI
GenAris: Generating Synthetic Iris Biometrics for Presentation Attack Security and Security for Generative Biometric Models	Mason	$33,333	VT
EPIC SWaPD: Energy Preserving IoT Cryptography for Small Weight and Power	Mason	$150,000	DARPA

Project Title	Lead Institution	Funding Amount	Funding Agency
WISPER: IUCRC Phase One George Mason University	Mason	$150,000	NSF
Spectrum Sharing	Mason	$50,000	NSF
Evaluation Services for Step Ahead 2.0 – Housing First Support Services	Mason	$82,598	FFC
Enhancing Cybersecurity Education	Mason	$98,101	DoC
Enhancing Cybersecurity Education	Mason	$101,800	DoC
Unifying Millimeter-wave Networking and Sensing using Commodity Backscatter	Mason	$239,332	NSF
Millimeter-wave Networking in Transient Topologies	Mason	$141,484	DoD
DELTA FORCE: Digital Environments for Life-Cycle Test and Evaluation For Off-Road Combat Vehicles	Mason	$1,640,000	DoD
MEADOW: Management Environment and Algorithms for Distributed Optimal Workflows	Mason	$52,500	ARFL
Systems Engineering	Mason	$81,097	DoD

Project Title	Lead Institution	Funding Amount	Funding Agency
AI Defense for Students	Mason	$112,000	Griffiss
Deep Learning and Experimentation for Property-Controlled Molecule Generation	Mason	$202,242	NSF
AFCENT Applied Research 2	Mason	$2,236,800	ARFL
AI in Education	Mason	$30,000	NSF
Reference-based Auto Security Patch Generation	Mason	$468,734	ONR
EAGLE: Empowering American Government Leadership in Cybersecurity through Education	Mason	$1,299,455	NSF
TRACER	Mason	$15,000	NSSC
Cyber Literacy	Mason	$1,963	CDAO
Literacy Prototype I	Mason	$781,916	CDAO
Literacy Prototype II	Mason	$10,234,750	CDAO
Literacy Prototype III	Mason	$9,651,083	CDAO
AB Immersion	Mason	$500,000	CDAO
Advisory for Ivory Coast	Mason	$650,000	CIT

Project Title	Lead Institution	Funding Amount	Funding Agency
ARCHER Integration Support 1	Mason	$10,000	FHWA
Security Provenance Tracking, Product Integrity, and Supply Chain Traceability for Additive Manufacturing	Mason	$328,000	DoE
ARCHER Integration Support 2	Mason	$98,000	FHWA
STAR TREC: Secure Telecommunications Architecture for Trusted and Resilient Electric Communications	Mason	$290,779	DoE
Culturally Adaptive Social Robot Navigation	Mason	$795,899	NSF
End-to-End Resilience in Autonomous Driving Systems: Strategic Vulnerability Assessment and Mitigation	Mason	$338,535	NSF
MELIOREM: An Integrated Evaluation Cyberinfrastructure towards Safe and Dependable Autonomous Systems	Mason	$279,674	NSF
AI4EDU: Cloud Infrastructure-Enabled Training for AI in Educational Research and Assessment	Mason	$184,360	NSF
Toward Understandability and Interpretability for Neural Language Models of Source Code	Mason	$107,712	NSF

Project Title	Lead Institution	Funding Amount	Funding Agency
Fostering Mathematical Modeling Competencies through Collaborative Learning in a Large Language Model Simulated Virtual Classroom	Mason	$578,047	NSF
Hardening Cybersecurity for mmWave Massive MMO 5G Networks at Physical Layer	Mason	$50,527	ARO
mmWave Testbed Support	Mason	$76,000	Army
Communications and Network Security (IEEE)	Mason	$24,000	NSF
Advancing Multi-User Virtual Reality Classrooms to Support Collaborative Experiential Learning and Teaching	Mason	$899,526	NSF
Adapting Mixed Reality Training Programs to Real-World Scenes to enhance Human-AI Teaming in Emergency Responses	Mason	$299,861	NSF
SBIR: Aerial Systems	Mason	$250,000.27	USAF
Total		**$36,675,861**	

Southwest Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
Assessment and Optimization of Human Performance in Mixed Reality Attacks	Virginia Tech	$1,053,119	DARPA
Byzantine Resilient Federated Learning in Sporadically Connected Wireless Networks	Virginia Tech	$900,000	Office of Naval Research
Cognitive Digital Twin for the Development of Secure and Resilient Smart Grid Cyber-Physical Systems	Virginia Tech	$610,000	Department of Energy
Collaborative Research: GCR Mineral Detection of Dark Matter	Virginia Tech	$2,277,792	National Science Foundation
Complex Reasoning and Planning with Multi-Agent LLMs for Diverse Real-World Tasks	Virginia Tech	$75,000	Cisco Research
Developing Real Time Simulator Models of inverter based resources (IBR)	Virginia Tech	$35,000	EPRI
Efficient Distributed Training with Coding	Virginia Tech	$100,000	Amazon
Embodied Optimization for Decision-Making in Dynamic and Uncertain Environments	Virginia Tech	$454,953	National Science Foundation
CAREER: Accelerating Algorithms for Computing Isogenies and Endomorphisms of Supersingular Elliptic Curves	Virginia Tech	$458,572	National Science Foundation
Intrusion Response Systems for Autonomous Vehicles with Human-Machine Teaming	Virginia Tech	$240,000	US Army Research Office
IUCRC Phase I Virginia Tech: Center for Cyber Science, Management, Applications, Regulation, and Training (Cyber SMART)	Virginia Tech	$200,000	National Science Foundation
Long Tailed Learning in the Open and Dynamic World: Theories, Algorithms, and Applications	Virginia Tech	$600,000	National Science Foundation
Modeling and Simulation Efficiency Improvements in End-to-End Electrical System Models	Virginia Tech	$591,000	Google

Project Title	Institution	Funding Amount	Funding Agency
Network-aware Multi-omics Large Language Model for Disease Progression Prediction	Virginia Tech	$5,000	National Science Foundation NAIRR Pilot
Prototype Development for Ultrafast Scheduler Integration into O-RAN	Virginia Tech	$50,000	LINK+LICENSE+ LAUNCH
Quantum Utility with hardware- and application- Informed Near-Term Algorithms (QUINTA)	Virginia Tech	$3,400,000	Department of Energy
Reasoning Over Long Context with Large Language Models	Virginia Tech	$100,000	Amazon AGI
SaTC: CORE: Small: A Framework for Safety Assurance in Foundation Models	Virginia Tech	$500,000	National Science Foundation
SaTC: CORE: Small: Securing Gaze Data from Side-Channel Attacks in Foveated Systems	Virginia Tech	$600,000	National Science Foundation
Collaborative Proposal: RAPID: Wildfire Resilience On Hawaiian Islands: Risk-Aware EmergeNcy PArtial Microgrid Shutoff (OHANA)	Virginia Tech	$80,000	National Science Foundation
Secure Telecommunications ARchitecture for Trusted and Resilient Electric Communications (STAR TREC)	Virginia Tech	$680,000	Department of Energy
Surveying implementation tradespace for post-quantum cryptographic algorithms	Virginia Tech	$32,000	Raytheon Technologies
Towards Safe and Robust Agentic AI for the Open Web	Virginia Tech	$60,000	Google
Trustworthy QA: Enhancing Complex Reasoning in Large Language Models	Virginia Tech	$25,000	National Science Foundation NAIRR Pilot
Quantum Photonic Integrated Design Center (QuPIDC)	Virginia Tech	$570,000	Department of Energy EFRC
Topological Nano-Antennas for Secure and Compact Wireless Communication	Virginia Tech	$30,000	Virginia Microelectronics Consortium (VMEC)

Project Title	Institution	Funding Amount	Funding Agency
3D Printed Sensors For Continuous Soil Nitrate Measurement In Corn Fields with Poultry Litter as a Soil Amendment	Virginia Tech	$20,500	Virginia Corn Board
Collaborative Research: Breaking Information Sharing Barrier at Signal Level: A Learning-based Interference Mitigation for Pay-As-You-Go Spectrum Sharing	Virginia Tech	$400,000	National Science Foundation
Electronic Logging Device Technical Improvements Study	Virginia Tech	$794,999	Federal Motor Carrier Safety Administration
Modernizing Talent Management in Virginia, Maryland, and D.C. (MTM VMD): Co-creating An Accessible Route to Cybersecurity	Virginia Tech	$97,135	NIST
Hybrid Quantum Algorithms for Computationally Hard Problems	Virginia Tech	$38,000	Fujitsu Research of America
Analog Front End (AFE) of Self Mixing Interferometry (SMI) and MEMS based Eye Tracking	Virginia Tech	$270,000	Meta Platforms Inc
QUICK-SWARM: Quick Unmanned Identification and Control with Knowledge-based SWARM detection	Virginia Tech	$57,000	U. S. Department of Defense and A2 Labs LLC
Fellows Program	Virginia Tech	$420,000	Raytheon Technologies
Department of Defense Cyber Scholarships	Virginia Tech	$1,027,381	U. S. Department of Defense
IC Centers for Academic Excellence, year 5	Virginia Tech	$200,000	ODNI
Uncovering Secrets from Virtual Reality Headsets via Electromagnetic Side Channels	Virginia Tech	$5,000	4VA
SaTC: CORE: Medium: Distributed Computing in Effect: Towards Trustworthy, Resilient and Secure NextG Mobile Networks	Virginia Tech	$320,799	National Science Foundation
IUSE: ESL: Level 1: Visualization-enhanced undergraduate Wireless engineering education through problem- and	Virginia Tech	$399,884	National Science Foundation

project-based learning (Visualize-U-Wireless-Pro)			
IUSE: ESL: Level 1: Visualization-enhanced undergraduate Wireless engineering education through problem- and project-based learning (Visualize-U-Wireless-Pro)	Virginia Tech	$399,884	National Science Foundation
SaTC: TTP: Small: Deployable Behavior-driven Crypto-ransomware Detection Enabled by Practical Logging Strategies	Virginia Tech	$600,000	National Science Foundation
Leveraging ML for Advanced IRR Validation: Towards a More Secure Internet Infrastructure	Virginia Tech	$30,000	Comcast Innovation Fund
SMC IV	Virginia Tech	$1,099,932	U. S. Department of Defense
CAREER: Data to Models (D2M) - A domain-guided translation of sensor data to analytical structural models	Virginia Tech	$674,582	National Science Foundation
Co-Opting Crime: Examining the Interaction and Impact of Nation States and Criminal Ransomware Gangs	Virginia Tech	$125,000	Cyber Academic Engagement Office
ASPEN: Advanced Signal Processing Enhancement for Next-Generation Open Radio Units	Virginia Tech	$2,204,228	NTIA
Automotive Cybersecurity projects	Virginia Tech	$917,941	Portfolio
Total		**$23,429,817**	

Appendix 2: AI for Cybersecurity / Cybersecurity for AI Research Grants

Coastal Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Adaptive Intrusion Detection in IoT Networks Using LLM-Driven Behavioral Analysis and Deep Reinforcement Learning	Ned Moghim	Old Dominion University	$100,000
AI Powered Cyber Defense: Leveraging Transformer Models and eXplainable Reinforcement Learning methods for Advanced Intrusion Detection and Response System	Mohammad Ghasemigol	Old Dominion University	$100,000
All In One: A Multitask LLM-Based Vulnerability Detector with Conversational Assistance	Huajie Shao	William & Mary	$100,000
Secure and Privacy-Preserving Decentralized AI through Model Refine and Fully Homomorphic Encryption	Qianlong Wang	Old Dominion University	$100,000
Toward Integrated Security and Privacy Solutions for Multi-Modal AI	Daniel Takabi	Old Dominion University	$100,000
Study of Adversarial Attack Strategies on Autonomous Vehicles Equipped with LiDAR Sensors	Abhishek Phadke	Christopher Newport University	$100,000
Enhancing the Security of Large Language Models Against Persuasion-Based Jailbreak Attacks in Multi-Turn Dialogues.	Javad Rafiei Asl	Old Dominion University	$100,000
An Attack-Resilient and Self-Healing Cyber Defense System with Distributed Deep Reinforcement Learning	Ghang Zhou	William & Mary	$66,667
Cyber-Attack Resilient Distributed and	Rafael Diaz	Old Dominion University	$66,667

Explainable AI with Zero Trust Architecture			
Leveraging Large Language Models for Enhanced Software Security Analysis and Malware Detection	Yanhai Xiong	William & Mary	$50,000

Central Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Secure and Privacy-Conscious Threat Detection via Federated Learning and Graph Neural Networks	Wajih Ul Hassan	University of Virginia	$100,000
Privacy Preserving Federated IoT Learning for Smart Public Health Surveillance	Thang Dinh	Virginia Commonwealth University	$100,000
Deepfake Detection by leveraging Conditional Generative Adversarial Networks with Uncertainty Quantification	Yuichi Motai	Virginia Commonwealth University	$100,000

Northern Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Meta-Architecture Binary Code Analysis: Multi-ISDA Deep Learning Analysis Leveraging Single-ISA Data	Lannan Lisa Luo	George Mason University	$100,000
Threat Hunting System Enhancement by Generative AI and LLMs	Mohamed Gebril	George Mason University	$100,000
Leveraging Large Language Models for Enhanced Software Security Analysis and Malware Detection	Kun Sun	George Mason University	$50,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Knowledge-Enhanced Threat Detection With Large Language Models	Peng Gao	Virginia Tech	$100,000
GenA(eye)ris: Generating Synthetic Iris Biometrics for Presentation Attack Security and Security for Generative Biometric Models	Brendan David-John	Virginia Tech	$100,000
Intelligent and Secure Wireless Sensor System for Monitoring Cattle on Farms	Sook Shin	Virginia Tech	$100,000
An Attack-Resilient and Self-Healing Cyber Defense System with Distributed Deep Reinforcement Learning	Bo Ji	Virginia Tech	$33,333
Cyber-Attack Resilient Distributed and Explainable AI with Zero Trust Architecture	Zeb Bowden	Virginia Tech	$33,333

Appendix 3: Regional Node Research Grants FY2025

Central Virginia Node

Project Title	PI	Lead Institution	Grant Amount
A Privacy Preserving Framework for Supporting Disaster Planning and Response	Anil Vullikanti, Ph.D.	University of Virginia	$50,000
Spoofing-Resilient and Communication-Compatible MmWave Radar - Sensing for Autonomous Systems	Kun Qian, Ph.D.	University of Virginia	$50,000
Distributed Differentially Private Tabular Data Synthesis	Tianhao Wang, Ph.D.	University of Virginia	$50,000
Angle Driven Innovations for IRS Communication	Yanxiao Zhao, Ph.D.	Virginia Commonwealth University	$100,000
Epistemic Human-Robot Interaction for Every-day Collaborative Operations	Nicola Bezzo, Ph.D.	University of Virginia	$100,000
Secure Communication-Enabled Connected Autonomous Vehicles	Azim Eskandarian, Ph.D.	Virginia Commonwealth University	$100,000
Understanding the Vulnerability of Cyber-Physical Systems with Attack Paths Analysis with its Evaluation in UAV-IoT Networks	Jundong Li, Ph.D.	University of Virginia	$100,000
Safeguard Communications from Smart Health Devices with DNS-based Key Management Infrastructure	Yixin Sun, Ph.D.	University of Virginia	$100,000
Development and field implementation of a human-in-the-loop connected cruise control system focused on cybersecurity and commercialization	Brian Park, Ph.D.	University of Virginia	$100,000
Enhancing Human-Robot Collaboration through Mixed Reality Interactions	Joseph Shelton, Ph.D.	Virginia State University	$100,000
Securing Highly Integrated AI-Assisted Emergency Medical Services for Smart Cities	Homa Alemzadeh, Ph.D.	University of Virginia	$100,000
Total			**$950,000**

Northern Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Threat Hunting System Enhancement by Generative AI and LLMs	Mohamed Gebril	George Mason	
Leveraging Large Language Models for Enhanced Software Security Analysis and Malware Detection	Kun Sun	George Mason	
Total			**$150,000**

Southwest Virginia Node: FY25 Cybersecurity Research

Project Title	PI	Lead Institution	Grant Amount
Psychological Game Theory-Based Optimization Approaches and Virtualization Tools for Networked Computing Systems	Manish Bansal	Virginia Tech	$37,500
Virginia Tech Quantum Seminar Series	Edwin Barnes	Virginia Tech	$20,000
Bridging the Gap Between User Interface Security and CI/CD Workflows	Chris Brown	Virginia Tech	$37,500
Moving Target Defense for Continuous Operation in Mission-Critical Cyber-Physical Systems	Tridapat Chantem Mohammad Azab	Virginia Tech Virginia Military Institute	$37,500 $37,500
IrisSwap: A public research challenge on digital iris spoofing attacks	Brendan David-John	Virginia Tech	$37,500
Fundamentals of Geotagging Images and Videos Using Non-Unique Landmarks	Harpreet Dhillon	Virginia Tech	$37,500
Addressing Software Defects and Security Vulnerabilities in Smart Home Automations	Xinghua Gao	Virginia Tech	$37,500
Enhancing the Privacy of Users with Disabilities Through Transparent Web Advertisement	Muhammad Gulzar	Virginia Tech	$75,000
Secure Component Monitoring of Open FutureG Networks	Wenjing Lou	Virginia Tech	$75,000
Research Engagement	Gretchen Matthews	Virginia Tech	$50,000
Coding theory for modern secure communication	Gretchen Matthews	Virginia Tech	$75,000
Resilient Coordinated Control of Renewable-Based power Grid Under Cyberattacks (ROBOCYBER)	Ali Mehrizi Sani	Virginia Tech	$37,500
Hidden Within Bechtler Project	Agnieszka Miedlar	Virginia Tech	$10,000
Fortifying the Foundation: Bolstering Safety and Trust in Multimodal Foundation Models Through Risk, Attack, and Defense Analysis	Christopher Thomas	Virginia Tech	$75,000
Privacy-Preserving Digital Twin Generation for Electronic Health Records with Large Language Models	Xuan Wang	Virginia Tech	$37,500
Total			**$717,500**

Southwest Virginia Node: FY25 Global Engagement

Project Title	PI	Lead Institution	Grant Amount
UVA Wise Global Engagement Program	Karen Carter	University of Virginia's College at Wise	$10,000
Using Honeypots to Understand International Differences in Cybercrime	Thomas Dearden	Virginia Tech	$9,628
Brazil GEOINT Initiative Proposal	Andrew Foy	Radford University	$10,000
Virginia International Research on Technology and Unified Cybersecurity in Electric Systems (VIRTUE)	Ali Mehrizi Sani	Virginia Tech	$10,000
The 1st Workshop on Agentic AI for Science: Hypothesis Generation, Comprehension, Quantification, and Validation	Dawei Zhou	Virginia Tech	$10,000
Total			**$49,628**

Southwest Virginia Node: Security Scholars Program

Project Title	PI	Lead Institution	Grant Amount
Software Defined Radio and O-RAN for Mobile Distributed MIMO (dMIMO)	Lingjia Liu	Virginia Tech	$55,650
Graduate Research & Innovation Design: Secure Connectivity for REnewable Devices in the grid (GRID-SECURED)	Ali Mehrizi Sani	Virginia Tech	$47,427
Large Language Model for Access Control Policy Generation in Microservices or Cloud Computing	Peng Gao	Virginia Tech	$14,255
Total			**$117,332**

CCI Hub FY25 Annual Report

	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25	Mar-25	Apr-25	May-25	Jun-25	Actual YTD	Budget Balance YTD	Budgeted	FY25 Encumbered Funds	
568002 - CCI - Hub - Labor															$ 4,786,892.00		
Labor - Faculty & Staff*	$ 473,812	$ 324,883	$ 434,111	$ 328,087	$ 351,395	$ 348,437	$ 342,894	$ 387,179	$ 352,024	$ 366,069	$ 348,333	$ 193,677	$ 4,251,461	$ (112,474)	$ 4,138,987		
GRAs (included in amount above)													$ -	$ 547,905	$ 547,905		
Wages													$ -	$ -			
Graduate Tuition Remission		$ 76,913	$ 25,353	$ 5,950		$ 13,198				$ (250)		$ 153,370	$ 274,544	$ (274,544)			
Subtotal	**$ 473,812**	**$ 401,796**	**$ 459,464**	**$ 334,047**	**$ 351,395**	**$ 361,635**	**$ 342,894**	**$ 387,179**	**$ 351,774**	**$ 368,069**	**$ 501,703**	**$ 193,677**	**$ 4,526,005**	**$ 260,887**	**$ 4,786,892**	**$ -**	
Burn Rate	**10%**	**18%**	**28%**	**35%**	**42%**	**50%**	**57%**	**65%**	**72%**	**80%**	**91%**	**95%**	**95%**				
568003 - CCI - Hub - Facilities															$ -		
VTRC-A Rent		$ 378,015	$ (336,013)	$ (42,002)									$ -		$ -		
Subtotal	**$ -**	**$ 378,015**	**$ (336,013)**	**$ (42,002)**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	
568004 - Hub Operations															**$ 697,063.00**		
NCR Communications (IT/Servers)			$ 10,088										$ 10,088	$ 29,912	$ 40,000		
Copy/Print	$ 239		$ 1,478	$ 514							$ 712		$ 2,943	$ 2,057	$ 5,000	$ 152	
Travel - Ops Staff (Jenny, John, Alex, Lulz, Laure)	$ 1,654	$ 3,848	$ 1,727	$ 2,002	$ 9,490	$ 564	$ 3,497	$ 361	$ 3,372	$ 3,892	$ 4,731	$ 617	$ 36,353	$ (1,353)	$ 35,000	$ 2,644	
Supplies		$ 1,912	$ 400		$ 2,108	$ 577		$ 660		$ 11	$ 113		$ 5,782	$ 2,218	$ 8,000		
VTRC-A Rent	$ 39,818	$ (316,547)	$ 394,928	$ 84,004	$ 42,002	$ 42,002	$ 42,002	$ 42,002	$ 42,002	$ 42,002	$ 42,002	$ 42,002	$ 536,218	$ (32,198)	$ 504,020		
Misc. Operating Expenses	$ 730	$ 407	$ 1,300	$ 7,060	$ 260	$ 130	$ 13,969	$ 303	$ 4,459	$ 1,039	$ 1,728	$ 457	$ 31,852	$ (26,852)	$ 5,000	$ 93,509	
Subtotal	**$ 42,442**	**$ (312,379)**	**$ 409,922**	**$ 94,179**	**$ 53,859**	**$ 43,274**	**$ 59,467**	**$ 43,326**	**$ 49,833**	**$ 46,944**	**$ 49,286**	**$ 43,085**	**$ 625,236**	**$ (28,216)**	**$ 597,020**	**$ 96,816**	
Burn Rate	**7%**	**-45%**	**28%**	**39%**	**48%**	**55%**	**65%**	**78%**	**91%**	**98%**	**97%**	**104%**	**104%**				
568005 - Hub Communications															**$ 49,860.00**		
Publications & Info Graphics													$ -	$ 15,000	$ 15,000		
Website													$ -	$ 2,500	$ 2,500		
Branding						$ 143	$ 126	$ 13					$ 282	$ 1,218	$ 1,500		
Digital Asset Management Software													$ -	$ 5,000	$ 5,000		
Marketing & Social Media Software	$ 442	$ 588	$ 412	$ 288	$ 288		$ 576	$ 288	$ 288	$ 368		$ 288	$ 3,826	$ 1,974	$ 5,800		
Video & Photo													$ -	$ 10,000	$ 10,000		
IT	$ 1,700									$ 2,554	$ 643		$ 4,997	$ (4,997)	$ -		
Travel - Comms Staff (Michele, Kate, Lisa)												$ 631	$ 631	$ 2,869	$ 3,500		
Subtotal	**$ 2,142**	**$ 588**	**$ 412**	**$ 288**	**$ 288**	**$ 143**	**$ 702**	**$ 301**	**$ 288**	**$ 3,022**	**$ 643**	**$ 919**	**$ 9,736**	**$ 33,566**	**$ 43,300**	**$ -**	
Burn Rate	**5%**	**6%**	**7%**	**8%**	**9%**	**9%**	**11%**	**11%**	**12%**	**19%**	**20%**	**22%**	**22%**				
568006 - Hub Workforce Dev & Innov+Comm															**$ 1,046,354.00**		
Experiential Learning Program*****	$ 10,000							$ (17,283)			$ 399,214	$ 323,619	$ 715,550	$ (115,550)	$ 600,000		
CCI Incubator Support (CATAPULT)												$ 300,000	$ 300,000	$ (100,000)	$ 200,000		
Hub-led Workforce Development Program						$ 44,954	$ (14,977)						$ 29,977	$ 25,023	$ 55,000		
Internship Fair													$ -	$ 5,000	$ 5,000		
Cyber Fusion							$ 20,000		$ 5,000		$ -	$ -	$ 25,000	$ (5,000)	$ 20,000		
State-wide Entrepreneurship Program							$ 1,500					$ 2,500	$ 4,000	$ 71,000	$ 75,000		
Project Based Learning		$ 9,072	$ 4,525	$ 8,337	$ 8,065	$ 6,895		$ 2,278	$ 2,977	$ 2,748	$ 188	$ 2,669	$ 47,755	$ 27,245	$ 75,000		
Meetup to Startup													$ -	$ 2,200	$ 2,200		
Program Management		$ 428			$ 1,500								$ 1,928	$ 3,072	$ 5,000		
Travel - Workforce Staff (Sarah, Kendall)		$ 135							$ 497	$ 525		$ 2,145	$ 3,402	$ 1,598	$ 5,000	$ 3,525	
Subtotal	**$ 10,000**	**$ 9,635**	**$ 4,525**	**$ 8,337**	**$ 9,565**	**$ 51,850**	**$ 6,523**	**$ (15,006)**	**$ 8,474**	**$ 3,273**	**$ 399,402**	**$ 630,893**	**$ 1,127,612**	**$ (86,412)**	**$ 1,042,200**	**$ 3,525**	
Burn Rate	**1%**	**2%**	**2%**	**3%**	**4%**	**9%**	**10%**	**8%**	**9%**	**9%**	**48%**	**108%**	**108%**				
568007 - Hub Network & External Engagements															**$ 90,000.00**		
CCI Symposium													$ -	$ 75,000	$ 75,000		
Symposium Expenses	$ 1			$ 5,672			$ 247	$ 0	$ 1,034	$ 52,725	$ 10,151		$ 69,830	$ (69,830)	$ -		
Symposium Registration Revenue								$ (4,560)	$ (6,860)				$ (11,420)	$ 11,420	$ -		
Symposium Travel										$ 5,171	$ 2,851	$ 283	$ 8,305	$ -	$ -		
Catering & Visitor Support		$ 1,791	$ 7,990	$ 6,634	$ 2,027		$ 236	$ 474	$ 2,750	$ 208			$ 22,109	$ (7,109)	$ 15,000		
Subtotal	**$ 1**	**$ 1,791**	**$ 7,990**	**$ 12,307**	**$ 2,027**	**$ -**	**$ 483**	**$ (4,086)**	**$ (3,077)**	**$ 58,104**	**$ 13,002**	**$ 283**	**$ 88,824**	**$ 1,176**	**$ 90,000**	**$ -**	
Burn Rate	**0%**	**2%**	**11%**	**25%**	**27%**	**27%**	**27%**	**23%**	**19%**	**84%**	**98%**	**99%**	**99%**				
568008 - Hub Research															**$ 906,169.00**		
Fall Research Program**						$ 900,000				$ 50,000			$ 950,000	$ (50,000)	$ 900,000		
Pres PostDoc Prof Dev					$ 845		$ 4,267						$ 5,112	$ (112)	$ 5,000		
Travel		$ 71	$ 579	$ 2,487	$ 227				$ 820	$ 92	$ 2,518	$ 5,020	$ 11,814	$ (11,814)	$ -		
Misc. Expenses		$ 20	$ 51	$ 20	$ 20	$ 45	$ 40	$ 20	$ 9,336	$ 500		$ 20	$ 10,071	$ (10,071)	$ -		
Subtotal	**$ -**	**$ 91**	**$ 630**	**$ 2,507**	**$ 1,093**	**$ 900,045**	**$ 4,307**	**$ 20**	**$ 10,155**	**$ 50,592**	**$ 2,518**	**$ 5,040**	**$ 976,997**	**$ (71,997)**	**$ 905,000**	**$ -**	
Burn Rate	**0%**	**0%**	**0%**	**0%**	**0%**	**100%**	**100%**	**100%**	**102%**	**107%**	**107%**	**108%**	**108%**				
568009 - Hub Research Infrastruouture															**$ 31,292.00**		
CCI xG Testbed								$ 60		$ 1,707	$ -		$ 1,766	$ 28,234	$ 30,000		
Software	$ 5,442					$ 8,056	$ 6,325			$ 660			$ 20,483	$ (20,483)			
Hardware					$ 9,950	$ 2,185		$ 214	$ 59,099	$ 525			$ 81,974	$ (81,974)			
Supplies		$ 4,149	$ 447	$ 2,006	$ 312	$ 1,000	$ 466	$ 543	$ 301	$ 13	$ 48		$ 9,288	$ (9,288)			
Phone	$ 52	$ 52	$ 52	$ 52	$ 173	$ 272	$ 122	$ 122	$ 122	$ 122	$ 122	$ 122	$ 1,386	$ (1,386)			**FY25 Total Spending & Burn Rate**
Subtotal	**$ 5,494**	**$ 4,201**	**$ 499**	**$ 2,058**	**$ 10,435**	**$ 11,513**	**$ 6,915**	**$ 939**	**$ 59,522**	**$ 3,027**	**$ 170**	**$ 122**	**$ 114,896**	**$ (84,896)**	**$ 30,000**	**$ -**	
Burn Rate	**18%**	**32%**	**34%**	**41%**	**78%**	**114%**	**137%**	**140%**	**372%**	**382%**	**383%**	**383%**	**383%**				
FY25 Total Executed and Encumbered	**$ 533,891**	**$ 483,737**	**$ 647,429**	**$ 412,321**	**$ 428,822**	**$ 1,388,459**	**$ 421,291**	**$ 412,874**	**$ 488,989**	**$ 531,191**	**$ 966,724**	**$ 874,059**	**$ 7,497,306**	**$ (87,147)**	**$ 7,500,000**	**$ 99,841**	**$ 7,587,147**
FY25 Burn Rate	**7%**	**14%**	**21%**	**26%**	**32%**	**50%**	**56%**	**61%**	**68%**	**75%**	**88%**	**100%**	**100%**			**1%**	**101%**

CCI Central Node FY25 Annual Report

	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25	Mar-25	Apr-25	May-25	Jun-25	Actual YTD	Budget Balance YTD	Budgeted	FY24 Encumbered Funds YTD
Operations																
Personnel	$ -	$ -	$ -	$ -	$ 125,000	$ -	$ -	$ -	$ -	$ -	$ -	$ 26,097	$ 151,097	$ 128,903	$ 280,000	$ 218,944
CVN Operations	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 420	$ -	$ 728	$ 2,315	$ 3,463	$ 146,537	$ 150,000	$ 180,398
UVA Program Support	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 125,000	$ 125,000	
Community Outreach/Events	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 50,000	$ 50,000	
Subtotal	$ -	$ -	$ -	$ -	$ 125,000	$ -	$ -	$ -	$ 420	$ -	$ 728	$ 28,412	$ 154,560	$ 450,440	$ 605,000	$ 399,342
Burn Rate	0%	0%	0%	0%	21%	21%	21%	21%	21%	21%	21%	26%	26%			
Workforce Development & Commercialization																
WFD CFP	$ -	$ -	$ -	$ -	$ 150,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 150,000	$ -	$ 150,000	
Interships in CVN	$ -	$ -	$ -	$ -	$ 75,000	$ -	$ -	$ -	$ -	$ -	$ 2,040	$ 18,440	$ 95,480	$ 54,520	$ 150,000	$ 41,410
Commercialization to CVN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 20,000	$ 20,000	
Commercialization to VCU	$ -	$ -	$ -	$ -	$ -	$ 2,911	$ (2,911)	$ -	$ -	$ -	$ -		$ -	$ 50,000	$ 50,000	
Commercialization to UVA	$ -	$ -	$ -	$ -	$ 50,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 50,000	$ -	$ 50,000	
CVN Partnerships	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 100,000	$ 100,000	
Subtotal	$ -	$ -	$ -	$ -	$ 275,000	$ 2,911	$ (2,911)	$ -	$ -	$ -	$ 2,040	$ 18,440	$ 295,480	$ 224,520	$ 520,000	$ 41,410
Burn Rate	0%	0%	0%	0%	53%	53%	53%	53%	53%	53%	53%	57%	57%			
Research & Investment																
Support Existing Programs	$ -	$ -	$ -	$ -	$ 150,000	$ -	$ 8,771	$ 2,708	$ 3,305	$ 1,671	$ 8,036	$ 8,073	$ 182,564	$ 267,436	$ 450,000	$ 89,746
Research Faculty	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 125,000	$ 125,000	
Research CFPs	$ -	$ -	$ -	$ -	$ 800,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 800,000	$ -	$ 800,000	
Subtotal	$ -	$ -	$ -	$ -	$ 950,000	$ -	$ 8,771	$ 2,708	$ 3,305	$ 1,671	$ 8,036	$ 8,073	$ 982,564	$ 392,436	$ 1,375,000	$ 89,746
Burn Rate	0%	0%	0%	0%	69%	69%	70%	70%	70%	70%	71%	71%	71%			
FY25 Total Executed and Encumbered	$ -	$ -	$ -	$ -	$ 1,350,000	$ 2,911	$ 5,860	$ 2,708	$ 3,725	$ 1,671	$ 10,804	$ 54,925	$ 1,432,604	$ 1,067,396	$ 2,500,000	$ 530,499
FY25 Burn Rate	0%	0%	0%	0%	54%	54%	54%	54%	55%	55%	55%	57%	57%			

YTD Executed & Encumbered	$ 1,963,102.56

DESCRIPTION	CODE	Jul 2024	Aug 2024	Sep 2024	Oct 2024	Nov 2024	Dec 2024	Jan 2025	Feb 2025	Mar 2025	Apr 2025	May 2025	Jun 2025	Total
REVENUE														
Registration Fee	3111	$0.00	$0.00	$0.00	$2,000.00	$180.00	$80.00	$4,100.00	$160.00	$380.00	$0.00	$30.00	$0.00	$6,930.00
Reciepts Other State Agency	3501	$0.00	$0.00	$0.00	$413,601.33	$0.00	$208,333.33	$624,999.99	$408,333.33	$13,893.35	$625,000.00	$247,525.82	$208,333.34	$2,750,020.49
Total Revenue		**$0.00**	**$0.00**	**$0.00**	**$415,601.33**	**$180.00**	**$208,413.33**	**$629,099.99**	**$408,493.33**	**$14,273.35**	**$625,000.00**	**$247,555.82**	**$208,333.34**	**$2,756,950.49**
EXPENSES														
LABOR														
Administrative Salaries	4001	$8,918.76	$13,378.14	$8,918.76	$4,459.38	$12,544.81	$8,918.76	$8,502.09	$8,918.76	$8,918.76	$4,459.38	$13,378.14	$4,459.38	$105,775.12
Classified Salaries	4002	$0.00	$5,400.01	$5,181.83	$1,966.67	$5,900.01	$1,966.67	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$20,415.19
Faculty Salaries	4005	$7,057.40	$73,694.37	$69,205.59	$37,375.84	$16,012.00	$89,583.01	$89,418.34	$89,418.34	$89,418.34	$44,000.83	$121,377.51	$5,149.16	$731,710.73
IT Salaries	4011	$7,938.26	$11,907.39	$7,938.26	$3,969.13	$15,876.52	$7,938.26	$7,938.26	$7,938.26	$7,938.26	$3,969.13	$11,907.39	$0.00	$95,259.12
Student w/o FICA	4025	$0.00	$0.00	$875.00	$987.50	$2,887.50	$937.50	$462.50	$2,012.50	$17,500.00	$1,087.50	$2,587.50	$0.00	$29,337.50
Wages	4031	$0.00	$3,000.00	$0.00	$0.00	$0.00	$20,500.00	$1,875.00	$1,875.00	$3,125.00	$1,250.00	$14,225.00	$1,250.00	$47,100.00
Moving & Relocation	4032	$0.00	$15,101.00	$0.00	$0.00	$0.00	$1,384.08	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$16,485.08
Awards/Honorariums	4034	$0.00	$0.00	$0.00	$1,384.08	$12,316.15	$1,384.08	$0.00	$0.00	$4,050.21	$4,152.24	$0.00	$0.00	$23,286.76
Bonus	4036	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$5,000.00	$15,062.56	$20,062.56
Mobile Device Allowance	4041	$90.00	$135.00	$90.00	$45.00	$135.00	$90.00	$90.00	$90.00	$90.00	$45.00	$135.00	$45.00	$999.00
Labor Total		**$24,004.42**	**$122,615.91**	**$92,209.44**	**$50,187.60**	**$65,671.99**	**$131,237.28**	**$108,286.19**	**$110,252.86**	**$131,040.57**	**$58,964.08**	**$168,610.54**	**$25,966.10**	**$1,089,046.98**
BENEFITS														
Employer Retire Cont-VRS Def Ben	4901	$1,510.09	$4,887.85	$3,649.84	$1,561.85	$4,685.55	$2,382.63	$3,528.51	$3,528.50	$3,528.50	$1,764.25	$5,292.75	$914.27	$37,234.59
FOAI SALARIED STATE EMP	4902	$5,089.56	$9,847.89	$5,668.15	$2,636.05	$7,957.30	$7,441.83	$6,626.95	$7,050.64	$7,147.08	$3,505.21	$11,862.17	$4,381.63	$79,214.46
Federal Old-Age Insurance for Wage	4903	$0.00	$0.00	$3.83	$0.00	$271.43	$80.33	$0.00	$0.00	$0.00	$0.00	$22.95	$0.00	$378.54
GROUP LIFE INSURANCE	4904	$251.71	$924.16	$943.02	$888.21	$1,732.43	$1,051.67	$1,348.47	$1,254.06	$1,254.06	$677.18	$1,730.64	$160.22	$12,215.83
HOSPITALIZATION INSURANCE	4905	$13,166.82	$16,813.77	$14,189.18	$8,280.09	$20,226.27	$13,066.68	$13,366.18	$13,366.18	$13,366.18	$7,385.09	$17,943.27	$5,597.09	$156,766.80
Teachers Insurance and Annunity	4906	$1,034.44	$1,707.90	$2,327.62	$878.67	$4,008.76	$2,335.34	$3,635.34	$2,855.34	$2,855.34	$1,379.50	$4,343.22	$1,137.78	$28,499.25
VSRS HEALTH CARE	4908	$223.95	$877.17	$895.07	$843.04	$1,644.32	$998.18	$1,279.89	$1,190.28	$1,190.28	$642.74	$1,642.62	$152.07	$11,579.61
L/T DISABILITY INSURANCE	4920	$62.11	$195.21	$124.76	$62.38	$187.14	$95.17	$107.60	$107.60	$107.60	$53.80	$161.40	$19.85	$1,284.62
CASH MATCH EXPENSE	4925	$134.94	$202.39	$134.93	$67.46	$202.38	$134.92	$134.92	$174.93	$174.93	$87.46	$262.38	$87.46	$1,799.10
VA HYBRID RETIREMENT ICMA/RC	4926	$1,845.76	$1,090.96	$77.04	$35.02	$110.37	$28.02	$136.71	$136.70	$136.70	$68.35	$205.05	$68.35	$3,939.03
VRS DCP Optional Retirement	4930	$0.00	$1,649.80	$1,665.72	$3,666.20	$4,198.56	$2,799.04	$2,799.04	$2,799.04	$2,799.04	$1,399.52	$3,798.19	$1,172.54	$28,746.69
	4997	$23,319.38	$38,197.10	$29,679.16	$0.00	$741.62	$0.00	$30,164.57	$29,664.23	$29,760.67	$15,563.58	$43,466.45	$13,691.26	$254,248.02
Benefits Total		**$23,319.38**	**$38,197.10**	**$29,679.16**	**$15,252.77**	**$41,025.95**	**$30,413.81**	**$30,164.57**	**$29,664.23**	**$29,760.67**	**$15,563.58**	**$43,466.45**	**$13,691.26**	**$340,198.93**
TRAVEL														
Personal Vehicle	7102	$0.00	$125.00	$182.19	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$307.19
Subsistance & Lodging	7105	$0.00	$1,021.87	$355.77	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$1,377.64
Meals	7107	$0.00	$0.00	$0.00	$0.00	$0.00	$10.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$10.00
Employer Travel/Lodging/Meals	7109	$4,345.21	$3,431.49	$535.89	$107.50	$107.50	$107.50	$107.50	$107.50	$107.50	$107.50	$107.50	$107.50	$9,280.09
Travel Total		**$4,345.21**	**$4,578.36**	**$1,073.85**	**$1,272.85**	**$285.69**	**$832.38**	**$208.00**	**$0.00**	**$0.00**	**$416.00**	**$2,249.50**	**$2,123.01**	**$17,384.85**
NPS														
Freight/Express	5001	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$240.00	$0.00	$240.00
Printing Services	5005	$893.63	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$893.63
Telephone Equip	5006	$43.00	$43.00	$43.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$129.00
Organization Memberships	5101	$2,500.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$2,500.00
Publication Subscriptions	5102	$0.00	$0.00	$0.00	$0.00	$639.41	$0.00	$0.00	$1,192.10	$748.80	$1,216.65	$0.00	$16,615.00	$20,411.96
Employee Training/Conferences	5103	$595.22	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$595.22
Employee Training and Consulting Services	5105	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$63,898.76	$3,765.00	$0.00	$0.00	$1,125.00	$68,788.76
Bank Service Charge	5213	$0.00	$0.00	$0.00	$0.00	$62.77	$7.95	$4.20	$139.95	$0.00	$0.00	$0.00	$0.00	$214.87
Food & Dietary Services	5404	$0.00	$647.64	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$647.64
Skilled Services-Firm	5414	$0.00	$0.00	$0.00	$4,245.94	$0.00	$228,234.30	$140,987.73	$177,432.00	$56,936.59	$29,086.99	$0.00	$18,070.90	$654,994.45
Computer Hardware Maint Serv	5455	$0.00	$383,114.56	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$2,556.00	$0.00	$0.00	$0.00	$385,670.56
Computer Software Maint. Svc.	5456	$0.00	$0.00	$0.00	$104.65	$0.00	$0.00	$74.62	$94.33	$26.14	$0.00	$217.96	$125.24	$642.94
Equipment Rentals (Copier)	5654	$0.00	$0.00	$0.00	$44.43	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$44.43
Grants to Non-govt Orgns	5580	$353,861.97	$383,114.56	$0.00	$4,245.94	$0.00	$228,234.30	$140,987.73	$177,432.00	$56,936.59	$29,086.99	$0.00	$18,070.90	$1,391,970.98
AMEX Purchases: Supplies	6101	$0.00	$0.00	$0.00	$4,502.52	$809.68	$228,359.75	$141,174.05	$242,864.64	$64,140.03	$30,411.14	$565.84	$36,043.64	$748,871.29
Plant Repair & Maintenance	6601	$0.00	$0.00	$0.00	$40.00	$182.19	$182.19	$208.00	$0.00	$0.00	$416.00	$216.00	$8.00	$1,252.38
Comp Operating Supplies	6803	$0.00	$0.00	$0.00	$582.66	$103.50	$650.19	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$1,336.35
Photography	6807	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$0.00	$2,033.50	$2,115.01	$4,148.51
NPS Total		**$357,893.82**	**$383,805.20**	**$43.00**	**$4,502.52**	**$809.68**	**$228,359.75**	**$141,174.05**	**$242,864.64**	**$64,140.03**	**$30,411.14**	**$565.84**	**$36,043.64**	**$1,490,613.31**

CCI Northern Node FY25 Annual Report

	Budgeted	Jul-24	Aug-24	Sep-24	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25	Mar-25	Apr-25	May-25	Jun-25	Actual YTD	Encumbered Funds	Budget Balance YTD	Budgeted
658002 - CCI - NoVa Node - Operations																	
Operations	$ 300,000	$ 16,305	$ 19,070	$ 14,608	$ 14,640	$ 15,116	$ 14,608	$ 18,262	$ 14,608	$ 19,320	$ 27,197	$ 30,200	$ 33,039	$ 236,974	$ 63,000	$ 26	$ 300,000
														$ -			
														$ -			
														$ -		$ -	
Subtotal	$ 300,000	$ 16,305	$ 19,070	$ 14,608	$ 14,640	$ 15,116	$ 14,608	$ 18,262	$ 14,608	$ 19,320	$ 27,197	$ 30,200	$ 33,039	$ 236,974	$ 63,000	$ 26	$ 300,000
Burn Rate		5%	12%	17%	22%	27%	31%	38%	42%	48%	58%	68%	79%	100%		0%	
658003 - CCI - NoVa Node - Research																	
Faculty Fellows	$ 400,000	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 8,333	$ 358,337	$ 450,000	$ -	$ (50,000)	$ 400,000
Research Proposals	$ 200,000	$ -	$ -	$ -	$ -	$ -	$ -	$ 150,000	$ -	$ -				$ 150,000	$ -	$ 50,000	$ 200,000
Undergraduate Research	$ 115,000	$ -	$ -	$ 20,800	$ 22,400	$ 23,200	$ 23,442	$ 15,158	$ 10,000	$ -	$ -	$ -	$ -	$ 115,000	$ -	$ (0)	$ 115,000
Contingency Support	$ 85,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 14,782	$ 18,400	$ 20,112	$ 17,600	$ 14,106	$ 85,000	$ -	$ 40,000	$ 125,000
Subtotal	$ 800,000	$ 8,333	$ 8,333	$ 29,133	$ 30,733	$ 31,533	$ 31,775	$ 173,491	$ 33,115	$ 26,733	$ 28,445	$ 25,933	$ 372,443	$ 800,000	$ -	$ 40,000	$ 840,000
Burn Rate		1%	2%	5%	9%	13%	17%	37%	41%	44%	48%	51%	96%	100%			
658005 - CCI - NoVa Node - Workforce Development																	
Subsidized Undergraduate Cybersecurity Internships	$ 310,000	$ 60,590	$ 30,160	$ 21,120	$ 21,120	$ 37,440	$ 21,730	$ 17,600	$ 21,120	$ 14,080	$ 16,720	$ 16,720	$ 25,600	$ 305,000	$ -	$ (5,000)	$ 300,000
Traineeships and Apprenticeships	$ 442,000	$ 147,600	$ 121,400	$ 64,000	$ 89,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 422,000	$ -	$ -	$ 422,000
Cybersecurity HS Internship & Essential Skills	$ 121,500	$ 38,300	$ 81,700	$ -	$ -	$ -	$ -	$ 1,500	$ -	$ -	$ -	$ -	$ -	$ 121,500	$ -	$ -	$ 121,500
Experiential Learning Sprints	$ 26,500	$ 2,159	$ 874	$ -	$ -	$ -	$ 1,943	$ 2,100	$ -	$ 1,282	$ -		$ 13,014	$ 21,372	$ -	$ 5,128	$ 26,500
														$ -			
														$ -			
Subtotal	$ 900,000	$ 248,648	$ 234,134	$ 85,120	$ 110,120	$ 37,440	$ 23,673	$ 21,200	$ 21,120	$ 15,362	$ 16,720	$ 16,720	$ 38,614	$ 869,872	$ -	$ 128	$ 870,000
Burn Rate		29%	56%	66%	79%	82%	85%	87%	90%	92%	94%	96%	100%	100%			
658006 - NoVa Node - Innovation																	
CCI Incubator + Accelerator (CATAPULT/CCI+A)	$ 500,000	$ 54,807	$ 68,428	$ 6,993	$ 10,159	$ 5,457	$ 206	$ -	$ -	$ -	$ 1,035	$ 303,104	$ 4,649	$ 454,838	$ 35,162	$ 0	$ 490,000
														$ -			
														$ -		$ -	
Subtotal	$ 500,000	$ 54,807	$ 68,428	$ 6,993	$ 10,159	$ 5,457	$ 206	$ -	$ -	$ -	$ 1,035	$ 303,104	$ 4,649	$ 454,838	$ 35,162	$ 0	$ 490,000
Burn Rate		11%	25%	27%	29%	30%	30%	30%	30%	30%	30%	92%	93%	100%			
FY25 Total Funds Executed	**$ 2,500,000**	**$ 328,094**	**$ 329,965**	**$ 135,855**	**$ 165,652**	**$ 89,548**	**$ 70,262**	**$ 212,953**	**$ 68,843**	**$ 61,415**	**$ 73,997**	**$ 375,957**	**$ 448,745**	**$ 2,361,884**	**$ 98,162**	**$ 40,154**	**$ 2,500,000**

CCI Southwest Node FY25 Annual Report

	Jul-24	Aug-23	Sep-24	Oct-24	Nov-24	Dec-24	Jan-25	Feb-25	Mar-25	Apr-25	May-25	Jun-25	Actual YTD	Budget Balance YTD	Budgeted
556020 - CCI SWVA - Node Research															
Research Projects		$ 829,832.00		$ -			$ 182,961.00	$ 10,000.00	$ 10,000.00			$ 10,000.00	$ 1,042,793.00	$ 18,201.00	$ 1,060,994.00
Research Personnel		$ 359,215.00	$ -	$ -	$ 85,000.00	$ -	$ -	$ -	$ -		$ -		$ 444,215.00	$ -	$ 444,215.00
Other													$ -	$ -	$ -
													$ -	$ -	
Subtotal	$ -	$ 1,189,047.00	$ -	$ -	$ 85,000.00	$ -	$ 182,961.00	$ 10,000.00	$ 10,000.00	$ -	$ -	$ 10,000.00	$ 1,487,008.00	$ 18,201.00	$ 1,505,209.00
Burn Rate	0%	79%	79%	79%	85%	85%	97%	97%	98%	98%	98%	99%	99%		
556021 - CCI SWVA - Node Innovation and Talent Pipeline															
Innovation Projects		$ 50,000.00		$ -			$ 50,000.00		$ 150,000.00	$ 51,000.00	$ -		$ 301,000.00	$ -	$ 301,000.00
Workforce Projects		$ 217,451.00	$ 1,000.00	$ 74,765.00			$ -		$ 1,500.00	$ -	$ 1,000.00	$ 122,000.00	$ 417,716.00	$ 4,575.00	$ 422,291.00
Innovation Personnel	$ 2,500.00	$ 8,000.00			$ -					$ 75.00	$ -		$ 10,575.00	$ (75.00)	$ 10,500.00
Outreach costs		$ -	$ -	$ 333.55	$ -	$ -	$ 10,000.00		$ 5,000.00	$ -	$ 159.90		$ 15,493.45	$ 9,506.55	$ 25,000.00
Internal CCI SWVA Interns			$ 513.24	$ 1,243.56	$ 1,314.60	$ 824.64	$ -	$ 530.79	$ 484.12	$ 661.83	$ 590.46		$ 6,163.24	$ 3,836.76	$ 10,000.00
Other													$ -	$ -	
Subtotal	$ 2,500.00	$ 275,451.00	$ 1,513.24	$ 76,342.11	$ 1,314.60	$ 824.64	$ 60,000.00	$ 530.79	$ 156,984.12	$ 51,736.83	$ 1,750.36	$ 122,000.00	$ 750,947.69	$ 17,843.31	$ 768,791.00
Burn Rate	0%	36%	36%	46%	46%	47%	54%	54%	75%	82%	82%	98%	98%		
556022 - CCI SWVA - Node Operations															
Labor	$ 60,393.55	$ 13,664.76	$ 13,640.27	$ 13,640.28	$ 13,600.27	$ 13,600.28	$ 13,640.28	$ 13,640.27	$ 13,640.28	$ 13,642.51	$ 13,644.77	$ 8,868.24	$ 205,615.76	$ 384.24	$ 206,000.00
Telecom	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	
Operating costs			$ -	$ -	$ 1,373.37	$ 137.67	$ 578.44		$ -	$ 738.10		$ 4,093.49	$ 6,921.07	$ 3,078.93	$ 10,000.00
Travel and Training Costs		$ 1,197.32	$ 957.82	$ -	$ 1,033.11	$ -		$ 500.00	$ -	$ 1,276.71		$ 199.00	$ 5,163.96	$ 4,836.04	$ 10,000.00
													$ -		
Subtotal	$ 60,393.55	$ 14,862.08	$ 14,598.09	$ 13,640.28	$ 16,006.75	$ 13,737.95	$ 14,218.72	$ 14,140.27	$ 13,640.28	$ 15,657.32	$ 13,644.77	$ 13,160.73	$ 217,700.79	$ 8,299.21	$ 226,000.00
Burn Rate	27%	33%	40%	46%	53%	59%	65%	72%	78%	84%	91%	96%	96%		
FY25 Total Executed and Encumbered	$ 62,893.55	$ 1,479,360.08	$ 16,111.33	$ 89,982.39	$ 102,321.35	$ 14,562.59	$ 257,179.72	$ 24,671.06	$ 180,624.40	$ 67,394.15	$ 15,395.13	$ 145,160.73	$ 2,455,656.48	$ 44,343.52	$ 2,500,000.00
FY25 Burn Rate	3%	62%	62%	66%	70%	71%	81%	82%	89%	92%	92%	98%	98%		

Bibliography

Virginia State Budget. (2018). Budget Bill - HB5002 (Chapter 2) [Accessed: 15 July 2020]. https://budget.lis.virginia.gov/item/2018/2/HB5002/Chapter/1/252/PDF/