



Fiscal Year 2026 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 2026 REPORT**

Commonwealth Cyber Initiative

September 29, 2026

Message from the Executive Director

The Commonwealth Cyber Initiative (CCI) is an unprecedented partnership between 47 institutions of higher education, working with industry and government agencies to advance cybersecurity. Much more than a traditional research center, CCI is an engine for economic development for Virginia, with interconnected missions of workforce development, innovation, and research.

Concerns related to Artificial Intelligence (AI)-identified cyber vulnerabilities and rogue AI agents keep making headlines, and cybersecurity is front and center in discussions around the development of quantum information sciences. This makes the focus area of CCI more relevant than ever. As with most academic research, Fiscal Year 2026 (FY26) has brought some headwinds in federal funding. Nevertheless, this year our researchers brought in \$49.2 million in new research grants and contracts, more than 50% above our annual baseline at the start of CCI. To address a rapidly evolving research funding landscape, we are leaning into our strategy of building research teams in the commonwealth that can be responsive to opportunities that require close collaboration with industry and relevant government agencies.

The job market for cybersecurity professionals remains very strong, a situation we expect to persist for the foreseeable future. More than ever, hands-on experience is an invaluable asset: our focus is on providing students with meaningful experiential learning opportunities at every stage of their academic journey. This year, 3,700 students went through CCI's experiential learning and career preparedness programs.

Ideas that are incubated in the lab increasingly form the foundation for new companies, new products, and new services. Our innovation programs support faculty and students in this transition, often pairing them with cybersecurity startups that can help bring this innovation to market.

We are proud of the return that CCI brings to the commonwealth's investment and hope that you will enjoy learning more about our activities in FY26 in this report.



Luiz DaSilva, Ph.D.; Fellow, IEEE; Senior Member, National Academy of Inventors; Member, Virginia Academy of Science, Engineering and Medicine
Executive Director, Commonwealth Cyber Initiative
Bradley Professor of Cybersecurity, Virginia Tech

Executive Summary

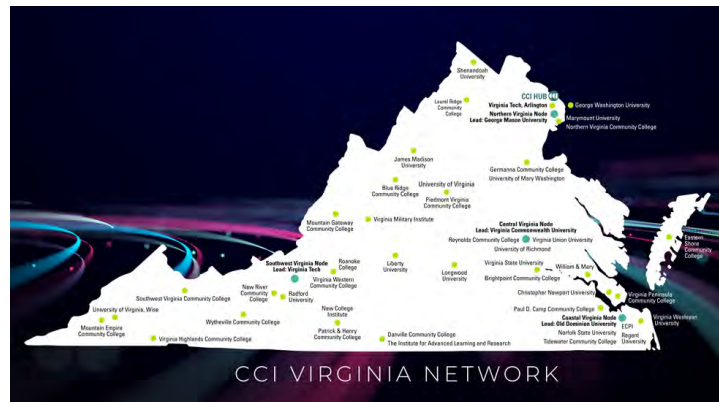
The Commonwealth Cyber Initiative (CCI) was established under the enabling authority of the Appropriation Act - Item 252.B7, Special Session I, 2018. Our objective is “to serve as an engine for research, innovation, and commercialization of cybersecurity technologies, and to address the commonwealth’s 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.

CCI remains unique in the nation by bringing together 47 higher education institutions with a common vision, articulated above, and a mission of research, innovation, and workforce development in cybersecurity. CCI also represents a unique example in the commonwealth of how inter-university collaboration can bring about an extremely robust return on investment, reflected in job creation, a significant increase in extramural research funding, the health of the cybersecurity startup system, and the ability to attract and retain talent. This report summarizes some of our key achievements in Fiscal Year 2026 (FY26).

Impact on the Commonwealth.

In six years of operation, CCI is recognized as a model for how statewide collaboration between higher education, the private sector, and government can result in economic impact for all. Even in a challenging research funding environment, our cybersecurity programs and research continue to thrive. In FY26 our researchers have attracted \$49.2 million dollars in new research grants and contracts. This success is a testament to the centrality of cybersecurity to national security and economic development, to the depth of research talent in Virginia, and to the strength of our multi-institution, transdisciplinary research teams. This year, 3,700 students participated in CCI workforce development programs designed to provide experiential learning and increase career preparedness. To date, we have launched 16 spinouts in Virginia. In 2025, Virginia startups attracted \$2.9 billion in venture capital, a record, and an estimated 27% of venture capital for the commonwealth is aligned with cybersecurity. CCI’s three mission lines continue to bring outstanding impact and return on the investment made by the commonwealth.



CCI's network of 47 higher education institutions.



CCI entrepreneurs and business partners attend a CATAPULT and ASCEND pitch event at George Mason University.

Node, we funded seven new teams in CATAPULT and six existing startups through ASCEND. CCI Nodes also run innovation programs targeting institutions in each geographic region, such as the Ideation to Commercialization program in Southwest Virginia (SWVA), Innovate Cyber Challenge in Coastal Virginia (CoVA), and the Project CYPHER-Bridge in Central Virginia (CVN). This year, we also partnered with Blu Ventures to help support its annual Cyber Ventures Forum. CCI's 16 spinouts, with founders from our network's faculty and students and receiving early support from CCI, hold 15 patents that form the intellectual property for their services and products.

Developing Cyber Talent. With an estimated 54,000 job openings in cybersecurity, and 112,000 professionals working in this field, Virginia continues to show extremely strong demand for cyber talent. Paradoxically, new graduates report finding it challenging to break into this job market. CCI's strategy is to provide students with experiential learning and career development opportunities, addressing the fact that even entry-level cybersecurity jobs expect some amount of work experience. In FY26, 3,700 students went through our programs. One example is Radford's Professional Accelerated Cyber Education (PACE) program, offering competency-based training for professionals across Virginia, which had 62 participants its first year. The team at Radford that designed and runs the program was recognized by our Technical Advisory Board with the CCI Impact Award 2026. Our project-based learning program, offering students micro-internships, continues to attract industry partners, including Microsoft, PBS, CACI, Guidepoint Security, and LMI. Through our Cyber As A Service program, more than 70 students have provided cybersecurity assessment and readiness services to small businesses in their communities. The number of internships curated (and sometimes subsidized) by CCI continues to grow. And the CCI NoVA Node's partnership with local high schools to provide internships to rising high school seniors and to recent high school graduates pursuing cybersecurity-related degrees is proving extremely popular.



Will Jedrzejczak, a graduating senior at James Madison University (JMU), talks about his experience in CCI's experiential learning program.



Julia Shapiro, doctoral student at Virginia Tech (VT), received this year's best poster award at our annual symposium.

Seeding External Research Funding.

CCI's seed grant programs show an estimated 7-to-1 return on investment: for each \$1 in seed funding, our researchers are able to attract \$7 in funding from sources outside the commonwealth. Seed grants are particularly impactful for junior faculty: in the last year, nine assistant professors supported by CCI, at William & Mary (W&M), the University of Virginia (UVA), Virginia Tech (VT), and George Mason University (Mason), have obtained prestigious CAREER awards from the National Science Foundation (NSF) in fields including computer science, physics, data science, and electrical and computer engineering. In FY26, CCI provided \$1.9 million in seed funding to multi-university teams working on securing our critical infrastructure. The Nodes provide additional seed funding to build research capacity in their regions. These pro-

grams advance the state-of-the-art in securing energy systems, water facilities, industrial control systems, transportation, manufacturing, healthcare, and communication networks. They were selected based on their intellectual merit and potential for follow-up funding from federal agencies and/or the private sector.

Cybersecurity across Borders.

Cybersecurity threats are borderless, and CCI's vision is to establish Virginia as a *global* leader in this field. We continue to build tight collaborations with researchers and institutions in like-minded countries. Japan's Ministry of Internal Affairs and Communications (MIC) has funded us to advise them on the establishment of an academia-government-industry partnership in cybersecurity in Japan, inspired by the CCI model. We have active research projects with Finland, Ireland, UK, and Japan, co-funded by NSF and funding agencies in those countries. In April 2026, we convened science attachés from 13 embassies to discuss potential collaborations with CCI. At that event, Virginia Economic Development Partnership (VEDP) talked about opportunities for international cyber companies seeking to establish a presence in Virginia. The SWVA Node of CCI organized a collaboration workshop in the Steger Center, in Switzerland, which concluded with a post-quantum cryptography event called Swissogeny Day, in partnership with IBM Zurich researchers. And this year, Luiz DaSilva chairs the board of the International Cybersecurity Center of Excellence (INCS-CoE), an organization bringing together universities from around the world to build partnerships in cybersecurity research and education.



Erdem Topsakal chaired a two-day workshop on AI and Cybersecurity in Istanbul, Türkiye, a partnership between CCI and MEF University.

Engaging with a Broad Array of Stakeholders. CCI engages with a broad array of stakeholders at the local, national, and international levels. We presented CCI in the annual meeting of RVA Connects, an organization with a mission of advancing economic prosperity and quality of life in the Richmond and Hampton Roads region. CCI was also featured in the annual summit of the Virginia Academy of Science, Engineering, and Medicine (VASEM), which this year focused on artificial intelligence. We led a fireside chat in the 2025 Times of Higher Education (THE) Innovation & Impact Summit, highlighting how CCI supports entrepreneurship in cybersecurity. These and numerous other engagements elevate Virginia's profile, showcase our strengths, and attract talent and businesses to the commonwealth. 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 CoVA, CVN, NoVA, and SWVA Nodes. And above all, the success of CCI is a result of the collaboration between more than 375 faculty members and thousands of students engaged in making Virginia a global leader in cybersecurity.



Luiz DaSilva talks to Sachin Shetty, professor in Old Dominion University (ODU), and Colin Dunn, of OP-SWAT, during the THE Innovation & Impact Summit.

List of Figures

1.1	The CCI network comprises 47 institutions of higher education across Virginia.	2
1.2	CCI governance structure.	2
1.3	Roles of the CCI Hub and Nodes.	3
1.4	CCI Leadership Council.	4
1.5	CCI organizational chart.	5
1.6	CCI xG testbed, indoors portion, in CCI Hub at VT.	5
1.7	Outdoor portion of the CCI xG testbed in Blacksburg, VA.	6
1.8	CCI xG testbed industry partners.	6
1.9	CVN In-kind support received in FY26.	7
1.10	CCI Technical Advisory Board (TAB).	8
1.11	Tom Bennett, Senior Director, Business Operations and Planning, with Svetlana Filiatreau, Senior Director, Business Development, of the IMPACT Lab at Radford University.	9
1.12	Website users by fiscal year	10
1.13	Social media followers for CCI's LinkedIn and Instagram accounts.	11
2.1	External funding obtained by the CCI network in FY26.	13
2.2	Critical Infrastructure Cybersecurity Research Program - Hub Funded	15
2.3	Critical Infrastructure Cybersecurity Research Program - Node Funded	15
2.4	FY26 - CVN Node Research Projects.	15
2.5	FY26 - NoVA Node Cybersecurity and Critical Infrastructure Research Projects	17
2.6	FY26 - NoVA Node Cybersecurity Supporting Industry-Faculty Collaboration Research Projects	18
2.7	FY26 - SWVA Node Cybersecurity Research Program.	19
2.8	FY26 - SWVA Node Research Engagement Program	20
2.9	FY26 - SWVA Node Additional Research Programs	20
2.10	FY26 - CoVA Node Agentic AI Cybersecurity and Security for Agentic AI Research Program	21
2.11	Dr. Daniel Takabi	22
2.12	Dr. Jacek Kibilda	23
2.13	Dr. Sam Noh	23
2.14	Dr. Sayanta Seth	24
2.15	SWVA Node New Faculty	25
2.16	CCI xG Testbed logo.	25
2.17	We showcase on our website some of the major findings and innovation produced by our researchers in FY26.	27
6.1	Geographic distribution of awards from appropriated funds.	66
1	CCI Hub FY26 Finance Report	96
2	Central Virginia Node FY26 Finance Report	97
3	Northern Virginia Node FY26 Finance Report	98
4	Southwest Virginia Node FY26 Finance Report	99
5	Coastal Virginia Node FY26 Finance Report	100

List of Tables

1.1	Mapping of reporting requirements to sections of this report.	12
-----	---	----

List of Acronyms

3GPP 3rd Generation Partnership Project

AI Artificial Intelligence

API Application Programming Interface

ASCEND Academic Support for Cybersecurity Entrepreneurship

CATAPULT Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology

CBRS Citizens Broadband Radio Service

CCI Commonwealth Cyber Initiative

CNU Christopher Newport University

CoVA Coastal Virginia

CTO Chief Technology Officer

CVN Central Virginia

FCC Federal Communications Commission

FY21 Fiscal Year 2021

FY22 Fiscal Year 2022

FY23 Fiscal Year 2023

FY24 Fiscal Year 2024

FY25 Fiscal Year 2025

FY26 Fiscal Year 2026

FY27 Fiscal Year 2027

GDP Gross Domestic Product

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

UMW University of Mary Washington

Mason George Mason University

NoVA Northern Virginia

NVCC Northern Virginia Community College

NSF National Science Foundation

NTIA National Telecommunications and Information Administration

ODU Old Dominion University

O-RAN Open Radio Access Network

OTIC Open Testing and Integration Center

PI Principal Investigator

RAN Radio Access Network

RoI Return on Investment

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

VSU Virginia State University

VT Virginia Tech

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

W&M William & Mary

xG Next Generation Networks

Contents

1	The Commonwealth Cyber Initiative	1
1.1	Vision and Mission	1
1.2	The CCI Network	1
1.2.1	Governance and network structure	1
1.2.2	CCI Hub Organization and Research Infrastructure Development	3
1.2.3	CCI Node Organization and Research Infrastructure Development	6
1.3	The CCI Technical Advisory Board	7
1.4	CCI Communications	9
1.4.1	CCI Social Media Strategy, Website, and Metrics	9
1.4.2	Appearances in the Media in FY26	11
1.5	Report Structure	12
2	CCI Research	13
2.1	External Grants to Support the Work of CCI	13
2.1.1	Extramural Funding in FY26	13
2.2	Research Grants Awarded from the Funds in HB30	13
2.2.1	Critical Infrastructure Cybersecurity	14
2.2.2	Node Funded Research Projects 2026	14
2.2.3	CVN Node	15
2.2.4	NoVA Node	16
2.2.5	SWVA Node	17
2.2.6	CoVA Node	20
2.2.7	CCI Fellows Program 2026	21
2.3	Faculty Recruited	23
2.3.1	Hub Faculty	23
2.3.2	Node Faculty	23
2.3.3	SWVA Virginia Node	23
2.4	CCI xG Testbed	24
2.5	Research Highlights and Breakthroughs	26
3	CCI Workforce Development	29
3.1	Hub-Led Programs	29
3.1.1	CyberFusion	29
3.1.2	Project-based Learning Program	29
3.1.3	Clearance Preparedness Program	29
3.1.4	Experiential Learning Program in FY26	30
3.1.5	Cyber As A Service	34
3.2	Node-led Programs	34
3.2.1	NoVA Node	34
3.2.2	CoVA CCI	36
3.2.3	SWVA Node	37
3.2.4	CVN Node	42

4	CCI Innovation	45
4.1	Hub-led Programs	45
4.1.1	Tech Transfer Support Fund	45
4.2	Node-led Programs	45
4.2.1	NoVA Node	45
4.2.2	SWVA Node	51
4.2.3	CVN Node	55
5	Collaborative Partnerships and Projects	56
5.1	Hub Partnerships	56
5.1.1	Industry-led Consortia	56
5.2	Node Partnerships	57
5.2.1	CVN Node	57
5.2.2	CoVA Node	58
5.2.3	NoVA Node	58
5.2.4	SWVA Node	59
5.3	Correlated Economic Outcomes	60
5.3.1	CCI Hub	60
5.3.2	CVN Node	60
5.3.3	NoVA Node	60
5.3.4	SWVA Node	61
6	Financial Report	63
6.1	CCI Hub	63
6.2	CCI Nodes	64
6.2.1	CoVA Node	64
6.2.2	CVN Node	64
6.2.3	NoVA Node	65
6.2.4	SWVA Node	66
6.3	Geographic distribution of the awards from Appropriated Funds	66
7	Looking Ahead: FY27	67
	https://www.overleaf.com/project/629f6db60ccb541ed76eb079	

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** with a focus on **cybersecurity**.

This report describes our progress in each of the mission lines in FY26, in pursuit of the vision of establishing the Commonwealth of Virginia as a global leader in cybersecurity. We also discuss how the investments in CCI have resulted in economic impact to the commonwealth.

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 Governance and network structure

The CCI network now comprises 47 institutions of higher education across Virginia, depicted in Figure 1.1. This level of statewide collaboration with a common mission of research, innovation, and workforce development in cybersecurity is unprecedented in the commonwealth and unique in the nation.

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 George Mason University (Mason), and the Southwest Virginia Node (SWVA) Node is led by VT. The CCI Hub is led by an Executive Director, assisted by the Deputy 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)

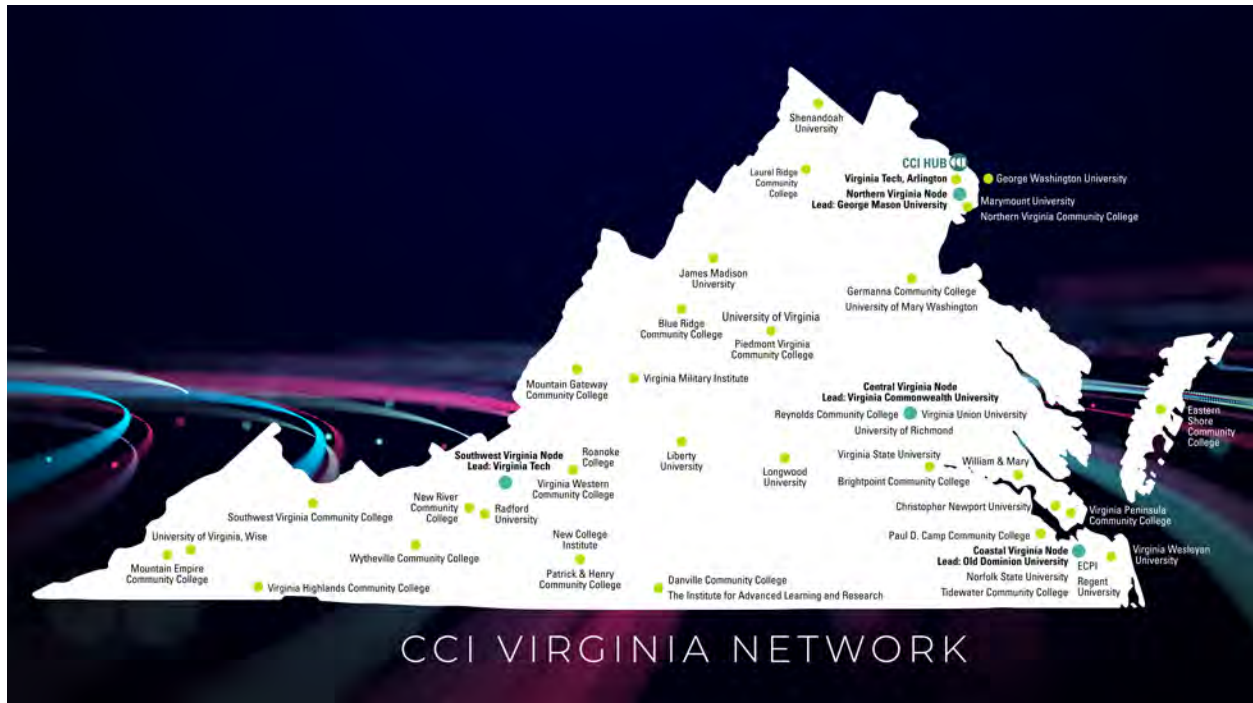


Figure 1.1: The CCI network comprises 47 institutions of higher education across Virginia.

provides oversight for CCI, as one of the commonwealth's centers of excellence. The governance structure is depicted in Figure 1.2.

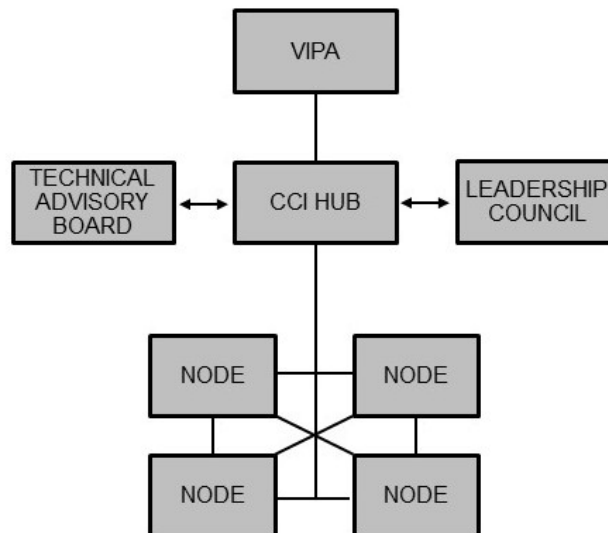


Figure 1.2: CCI governance structure.

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 Deputy 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 CoVA Node Director; he is also the Director of the School of Cybersecurity at ODU. Dr. Erdem Topsakal serves as CVN Director; he is also a professor 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 twice a year.

1.2.2 CCI Hub Organization and Research Infrastructure Development

The CCI Hub is led by the Executive Director. Prof. Jeff Reed, Willis G. Worcester Professor in the Department of Electrical and Computer Engineering at VT, serves as a special advisor to the Executive Director.

In May 2026, the CCI Hub underwent a reorganization designed to streamline the operations functions, better support the externally funded research conducted in the CCI Hub, and foster growth of our workforce development and innovation programs. Prof. Eric Burger, Research Professor at VT, has assumed the role of CCI's Chief Technology Officer (CTO), providing advice and leadership of the research focus areas of the initiative.

Mr. John Delaney, previously Managing Director of CCI, has transitioned to the role of Deputy Director. In that role, he represents CCI to all stakeholders when the Executive Director is unavailable to do so. He also leads a significant portion of the administrative team in the CCI Hub, including a Communications and Marketing Director, a Human Resources (HR) generalist, and a financial specialist.

A new Outreach Director is currently being recruited. That role, reporting to the CCI Executive Director,



Figure 1.4: CCI Leadership Council.

will lead a team responsible for our innovation and workforce development programs, with a strong focus on building partnerships with industry, government, and philanthropic organizations, procuring additional resources to expand these programs.

A new Research Director is currently being recruited. That role, reporting to the CCI Executive Director, will lead the work in extramural funded research in the CCI Hub, which has grown to around \$4 million in new research grants and contracts per year. The Research Director will also supervise the CCI Hub research faculty, the Director of CCI's xG testbed, and a grants manager responsible for the administrative and financial aspects of pre- and post-award funded research.

The organizational structure of the CCI Hub is shown in Figure 1.5.

The CCI Hub occupies dedicated space in VT'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 in 6G and beyond. 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. The testbed is accredited by the ORAN Alliance as an Open Testing and Integration Center (OTIC), allowing us to issue compliance and security badges and certifications to telecommunications vendors.

An outdoor component of the xG testbed is deployed in the Blacksburg campus of VT. This outdoor testbed offers unique opportunities for testing and validation of new wireless network technologies being developed for 6G and uses VT's Citizens Broadband Radio Service (CBRS) spectrum licenses. Three site locations have been selected around Stroubles Creek in Blacksburg, VA. We had an official launch of the outdoor testbed in the Fall of 2025, and these capabilities have already attracted significant funding from the private and the public sectors for outdoor experiments. The set-up and testing of components of the outdoor xG testbed can be seen in Figure 1.7.

While the original components of the xG testbed were acquired with CCI funds, for the past several years the testbed has attracted significant external investment. This includes \$5.64 million in equipment on

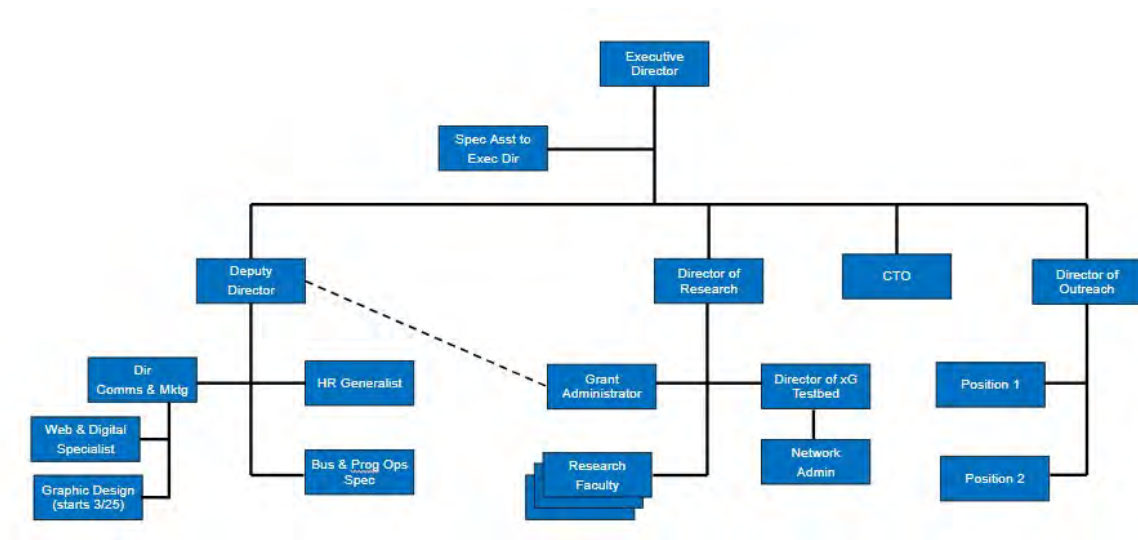


Figure 1.5: CCI organizational chart.



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



(a) Antennas in one of three sites of the outdoor testbed.



(b) Wireless experiments in the outdoor testbed.

Figure 1.7: Outdoor portion of the CCI xG testbed in Blacksburg, VA.



Figure 1.8: CCI xG testbed industry partners.

loan or donated by industry, and \$3.1 million in extramural funding for experimental research conducted by CCI researchers. Current industry partners of the testbed, which have provided in-kind and/or cash contributions, are depicted in Figure 1.8.

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.

For FY26, infrastructure development included VCU receiving an in-kind donation from IonQ Research for Quantum cloud computing credits, valued at \$5,000, which supported semi-quantum machine learning research. VCU also secured access to Rensselaer Polytechnic Institute’s IBM PAAM software-defined radio testbed, IBM’s D-Wave quantum annealing system, and Amazon Web Services with Booz Allen Hamilton’s AWS AI Academy instruction and materials.

In-Kind Financial Contributions				
PI	Institution	Contributor	Contribution	Value
Thang N. Dinh	VCU	IonQ Research	Quantum cloud computing credits supporting semi-quantum machine learning research	\$5,000

In-Kind Infrastructure and Resources		
Resource	Provider	What It Contributes
IBM PAAM software-defined radio testbed	Rensselaer Polytechnic Institute	Real-world experimental facility supporting Dr. Qian's beam management research; access provided through academic collaboration
D-Wave quantum annealing system access	D-Wave Systems / IBM	Quantum computing capability for benchmarking detection models in water infrastructure security research
AWS AI Academy instruction and materials	Amazon Web Services, with Booz Allen Hamilton	Five-day immersive AI and machine learning curriculum delivered to 35 UVA students

Figure 1.9: CVN In-kind support received in FY26.

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 FY26 are (Figure 2.15):

- Ms. Megan Samford, Vice President and Chief Product Security Officer for Energy Management, Schneider Electric;
- Prof. Anthony Tongen, Vice President and Chief Research Officer, 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).



(a) Ms. Megan Samford.



(b) Dr. Anthony Tongen.



(c) Prof. Sennur Ulukus.



(d) Ms. Tracy Gregorio.



(e) Mr. Jim Mollenkopf.



(f) Mr. Zachary Tudor.



(g) Mr. Dan Woolley.

Figure 1.10: CCI Technical Advisory Board (TAB).

The full TAB meets twice a year. FY26's Fall meeting, on October 16, 2025, was held in person at the VTRC-A, 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; presentations on the innovation mission line, including Catapult/ASCEND by Liza Wilson Durant, CCI's NoVA Node Director, Cyber Innovation Scholars by Gretchen Matthews, CCI's SWVA Node Director, and Chronosys, LLC, by Bahman Abolhassni, VT; presentations on the workforce development mission line, including Cyber 4n6 and CYPHER Bridge by Erdem Topsakal, CCI's CVN Node Director, the student-run Security Operations Center (SOC) and Cyber as a Service Program by Daniel Takabi, CCI's CoVA Node Director and Teresa Duvall, ODU, and the TEEM Program by Bobby Keener; as well as a research presentation, including information about the IUCRC WISPER, by Jacek Kibilda, VT. CCI's Deputy Director, John Delaney, shared an overview of CCI's annual report, economic impact report, and Virginia Works workforce development updates. Additional time was provided for an open discussion with advice from the TAB.

FY26's Spring meeting, held on March 23, 2026, 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; a presentation on the Critical Infrastructure Research Program by Kai Zeng, Mason; a presentation on SympleSolutions: A CCI Spinout Success Story and Mimetics by Carl Elks, VCU; a workforce development cybersecurity, data analytics, and AI panel discussion led by Gurkan Akalin, UVA Wise. Time for open discussion and advice from the TAB was also provided.

The TAB also formed a sub-committee to select the winner of the CCI Impact Award 2026. 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 Tom Bennett, Senior Director, Business Operations and Planning, with Svetlana Filiatreau, Senior Director, Business Development, of the IMPACT Lab at Radford University, for creating and implementing the Professional Accelerated Cyber Education (PACE) program, an online, self-paced, competency-based cybersecurity training model structured specifically for working professionals, and a full cybersecurity certificate stack. Under their leadership, CCI investment was transformed into durable outcomes that enhanced public-sector cyber resilience, expanded equitable access to high-quality cybersecurity education, and strengthened Virginia's position as a leader in applied, workforce-driven cybersecurity innovation (Figure 1.11).



Figure 1.11: Tom Bennett, Senior Director, Business Operations and Planning, with Svetlana Filiatreau, Senior Director, Business Development, of the IMPACT Lab at Radford University.

1.4 CCI Communications

1.4.1 CCI Social Media Strategy, Website, and Metrics

CCI's name recognition and stature are on the rise, a result of focused efforts throughout our mission lines.

CCI leadership is convening international cybersecurity experts to address global cyber issues. CCI-funded researchers are presenting at prestigious conferences, publishing notable research papers, and landing significant research grants. Our workforce development programs are connecting employers with talented students. Innovation programs are helping researchers become entrepreneurs and connecting startups with the research expertise they need to become successful companies.

Communications feature these activities and more on our website, through social media channels, and in our monthly newsletter, which is read by a highly engaged audience. We also create high-quality informational brochures and one-pagers, along with infographics and printed materials.

People want to know more about CCI. One clear indicator is our website traffic pattern.

Website Traffic

Direct traffic became the dominant growth engine in FY26, accounting for most of the increase in users and sessions. A surge in direct traffic likely indicates higher brand awareness, increased repeat visitation, and more users coming directly from bookmarks, saved links, and shared resources.

Direct/new users jumped 53.7 percent to 63,587 and direct/sessions increased 45.7 percent to 71,935 in FY26 from the prior year.

Website visitors are especially interested in our workforce development programs, proposal opportunities, and CCI Symposium content.

AI-driven discovery emerged as a meaningful new channel in FY26: platforms such as ChatGPT and other generative AI tools drove more than 1,600 sessions to our website, up from essentially none the prior year. Organic search remained a larger channel overall, bringing nearly 18,800 new users and more than 36,400 sessions to learn more about cybersecurity research, workforce development opportunities, funding announcements, and event information.

Our global reach is also expanding. People from more than 180 countries and territories, with a focus on Asia-Pacific and European markets, visited our website.

Total Website Users by Fiscal Year

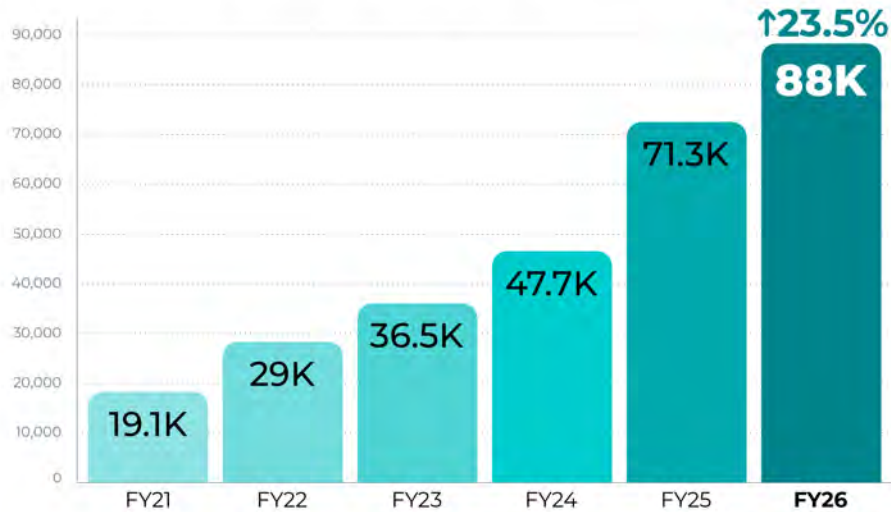


Figure 1.12: Website users by fiscal year

- Overall FY26 website users increased to 88,025, a 23.5 percent increase from the prior year.
- Website sessions grew to 120,208, a 15.4 percent increase.
- Clicks and other interactions increased to 613,880, a 15.47 percent increase.

Social Media

Social media outreach informs and brings people to our website. LinkedIn and Instagram anchor our social media strategy.

- LinkedIn grew to 4,794 followers, a 27.0 percent increase, while total impressions rose to 149,580, up 23.2 percent from the prior year.
- Instagram increased to 469 followers, a 37.5 percent increase, with total reach up more than fourfold to 5,330.
- Facebook grew to 210 followers, a 14.1 percent increase, and remains a smaller, secondary channel.

Across the year's 172 LinkedIn posts, CCI averaged a 9.8 percent engagement rate — well above the 2–5 percent typical range for company pages — that held up consistently across the year rather than being carried by one or two viral moments, pointing to a genuinely engaged, returning audience.

As a smaller, secondary channel, Instagram plays a different role: it's where CCI reaches general audiences outside the cybersecurity field, not just researchers and practitioners.

Outreach was driven in large part by three sustained campaigns: the 2026 CCI Symposium, the Research Paper Showcase, and the "Graduate Research Assistants: What's Next" series — each of which produced some of the year's highest-performing posts. These posts, which ran on LinkedIn and Instagram, were shared well beyond CCI's existing audience.

Figure 1.13 shows the evolution of our social media followers for our LinkedIn and Instagram accounts.

Research Paper Showcase and CyberArts

The communications team also leads programs connected to our mission lines.

The [2026 Research Paper Showcase](#) features the results of CCI funding through impactful peer-reviewed papers from high-level publications and conferences. The 22 papers advance cybersecurity research across artificial intelligence, privacy, cyber defense, emerging technologies, and human factors that shape a secure digital future.

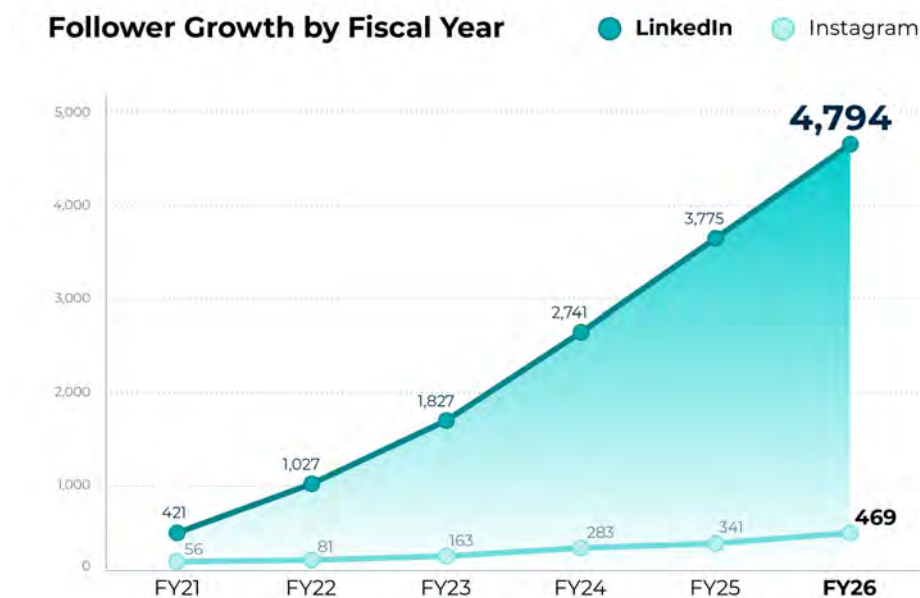


Figure 1.13: Social media followers for CCI's LinkedIn and Instagram accounts.

Looking ahead: CyberArts 2027 will challenge researchers and artists to reimagine cybersecurity impact. We began laying the groundwork in FY26, and we are working closely with the Institute of Creativity, Arts, and Technology at VT on the call for proposals and exhibit.

1.4.2 Appearances in the Media in FY26

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:

- [Seven Takeaways from CCI's European AI Cybersecurity Workshop](#) (Hub and CVN)
- CCI Builds Global Partnerships to Tackle Cyber Threats (Hub)
- International Collaboration Key to Addressing Cybersecurity threats (Hub)
- CCI Symposium 2026 Breaks Records in Attendance and Poster Presentations 277 attendees • 77 posters
- 7 demos • 41 paper presentations (Hub)
- Julia Shapiro Earns Best Poster Award at CCI Symposium 2026 (Hub and SWVA)
- The Commonwealth Cyber Initiative Expands Efforts to Protect Critical Infrastructure from Cyberattacks (Hub)
- CCI Helps Launch New Startups (Hub and NoVA)
- CCI Launches New Outdoor Wireless Test Bed (Hub)
- Radford University's Vinod Chachra IMPACT Lab Recognized with 2025 CCI Impact Award (Hub and SWVA)
- NSF Cyber SMART's Fall Meeting Shapes Fifth Year of Project, Legacy and Future Plans, And Adds New Member (Hub and SWVA)
- Students Test Cyber Skills, Connect with Employers at Commonwealth Cyber Fusion (Hub)
- To Fight Cybercrime, VCU Student Unravels the Layers Of 3D Printing (CVN)
- UVA Cyber Defense Team Outperforms Claude and Collegiate Rivals to Earn No. 2 National Ranking (CVN)
- VCU and CCI Central Node Launch New Ai Testbed (CVN)
- Building Virginia's Cyber Workforce through Cyber4n6 (CVN)
- Coastal Region Cybersecurity Hub Drives Innovation and Opportunities (CoVA)
- Old Dominion University Launches First Ph.D. in Cybersecurity in Virginia (CoVA)

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	5.3
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.

Secure AI Meets the Ocean: Student Fellows Help Chart the Future of Marine Science (CoVA)
 Securing Christopher Newport’s Standing in Cyberspace (CoVA)
 Virginia Universities Help Entrepreneurs Get Started (NoVA)
 CCI NoVA Node Promotes a Research Culture: part of series (NoVA)
 George Mason Team Wins Virginia Cyber Cup Competition at Commonwealth Cyber Fusion Event (NoVA)
 George Mason Students Ran with the Big Dogs at Defense Hackathon (NoVA)
 When A Cyberattack Hits the Physical World (SWVA)
 Cybersecurity Projects at Colleges and Universities Go from the Lab to the People (SWVA)
 Radford University Program Offers Cybersecurity Education to Working Professionals (SWVA)
 Cadets Helping Businesses Address Cybersecurity (SWVA)

1.5 Report Structure

This report describes the CCI’s progress and achievements in FY26. 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 is devoted to CCI’s collaborative partnerships and a discussion of the economic impact of our programs. Chapter 6 contains the financial reports from the Hub and Nodes for FY26. Finally, Chapter 7 describes our main activities and programs planned for Fiscal Year 2027 (FY27).

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 FY26 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 FY26

In FY26, the CCI network received 146 external grants totaling \$49,292,618 to support the CCI mission lines of research, workforce development, and innovation. 114 grants (80%) were from federal agencies and 32 (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	17	\$3,656,429
Central Virginia	9	\$5,917,868
Coastal Virginia	13	\$9,272,555
Northern Virginia	73	\$20,879,447
Southwest Virginia	34	\$9,566,319
Total	146	\$49,292,618

Figure 2.1: External funding obtained by the CCI network in FY26.

2.2 Research Grants Awarded from the Funds in HB30

In FY26, 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 Critical Infrastructure Cybersecurity

Objective of the Call

The focus of this call is to seek proposals for seed research grants that advance the state of the art of critical infrastructure cybersecurity. Topics include but are not limited to:

- 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.

Objectives of this call include:

- 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.

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 cybersecurity for critical infrastructure.
- 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 21 grants to CCI research teams throughout the commonwealth. The CCI Hub funded 19 grants. The NoVA Node funded 2 additional grants. 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.

2.2.2 Node Funded Research Projects 2026

In FY26, the CCI Regional Nodes awarded and funded 66 research programs totaling \$2,964,349 in research grants. The research projects focus on a wide range of cybersecurity topics, including supply chain security, artificial intelligence, smart technologies, the 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:

Node	Number of Grants	Grant Total
Central Virginia	4	\$400,000
Coastal Virginia	6	\$600,000
Northern Virginia	3	\$300,000
Southwest Virginia	6	\$594,000
Total	19	\$1,895,000

Figure 2.2: Critical Infrastructure Cybersecurity Research Program - Hub Funded

Node	Number of Grants	Grant Total
Northern Virginia	2	\$200,000
Total	2	\$200,000

Figure 2.3: Critical Infrastructure Cybersecurity Research Program - Node Funded

2.2.3 CVN Node

Title of the Research Program:

CVN Research Grant FY26

Objective of the Call:

To support projects aligned with CVN's research focus areas — cyber-physical systems, autonomous systems, Internet of Things as applied to medical device security, and smart city technology — producing novel research that advances CCI's mission.

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: 8

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	3	\$300,000
University of Virginia	5	\$500,000
Total	8	\$800,000

Figure 2.4: FY26 - CVN Node Research Projects.

2.2.4 NoVA Node

In FY26, the NoVA Node executed three major research calls for proposals, resulting in 11 grants awarded, totaling \$650,000 to support research capacity building at James Madison University (JMU) as they begin their strategic work to R1 status, critical infrastructure cybersecurity, and university-industry collaboration in general throughout the NoVA Node.

Title of the Research Program:

Research in Cybersecurity and Critical Infrastructure. Limited to researchers from JMU.

Focus of the Call:

The focus of this call for proposals is to advance the state of the art of cybersecurity for critical infrastructure, while specifically advancing JMU's research portfolio.

Objectives of the Call:

- To produce seminal contributions to our understanding of cybersecurity in the context of critical infrastructure – including chemical; commercial facilities; communications; critical manufacturing; water, wastewater, and dam systems; the defense-industrial base; emergency services; energy and nuclear reactors, materials, and waste; financial services; food and agriculture; government facilities; healthcare and public health; information technology; and transportation systems.
- To facilitate the impact of multiple disciplines, directly or indirectly related to, on cybersecurity challenges in the context of critical infrastructure.
- To position JMU-affiliated CCI researchers to be competitive for government and industry funding of research to fortify and secure cyber systems and address their role in critical infrastructure, as well as the resiliency of associated systems.

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 Cybersecurity and Critical Infrastructure.
- Feasibility and soundness of project plan in terms of achieving objectives, with requested and contributed resources, within the period of performance.
- Strength and relevance of academic expertise and any proposed contributions of academic partners to R&D project goals and deliverables.
- Economic impact on Commonwealth of Virginia.

Research Grants Awarded: 5

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

Title of the Research Program:

Research in Cybersecurity Supporting Industry-Faculty Collaboration

University	Number of Grants	Grant Total
James Madison	5	\$250,000
Total	5	\$250,000

Figure 2.5: FY26 - NoVA Node Cybersecurity and Critical Infrastructure Research Projects

Focus of the Call:

The focus of this call for proposals is to advance the state of the art of cybersecurity challenges faced by industry while catalyzing partnership and collaboration between industry and academic subject matter experts.

Objectives of the Call:

- Advance commercially relevant cybersecurity-related technologies, processes, algorithms, prototypes, or inventions to address cybersecurity challenges related to national defense, infrastructure security, transportation, electric/power distribution, manufacturing or resilience of cyber systems to human behavior.
- Leverage resources across industry/government and academia to reduce costs and accelerate technological advances.
- Facilitate and accelerate collaboration between CCI NoVA Node university faculty and industrial/government research enterprises within the Commonwealth of Virginia.
- Expand opportunities for academic faculty to engage in applied research.
- Expand industry/government awareness of academic expertise within NoVA.
- Position CCI NoVA Node researchers to be competitive for government and industry funding of research to fortify and secure cyber systems.

Selection Criteria

- Relevance to cybersecurity in CCI NoVA Node's strategic focus areas of national defense, infrastructure security, transportation, electric/power distribution, manufacturing or resilience of cyber systems to human behavior.
- Feasibility and soundness of project plan in terms of achieving objectives, with requested and contributed resources, and within period of performance.
- Feasibility and soundness of project plan in terms of achieving objectives, with requested and contributed resources, within the period of performance.
- Strength and relevance of academic expertise and proposed contributions of academic partners to R&D project goals and deliverables.
- Economic impact on Commonwealth of Virginia.

Research Grants Awarded: 4

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

2.2.5 SWVA Node

Title of the Research Program

FY26 Cybersecurity Research Program

University	Number of Grants	Grant Total
George Mason	4	\$200,000
Total	4	\$200,000

Figure 2.6: FY26 - NoVA Node Cybersecurity Supporting Industry-Faculty Collaboration Research Projects

Objective of the Call:

The Commonwealth Cyber Initiative (CCI) is establishing Virginia as a global center of excellence at the intersection of intelligence, autonomy, and security. With a mission of research, innovation, and workforce development, CCI serves as a catalyst for the commonwealth's long-term leadership in this sector through the collaboration of a central hub and four regional nodes. VT leads the CCI SWVA Node. 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 should be within the intersection of data, autonomy, and security. The CCI SWVA 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: 11

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
University of Virginia-Wise	1	\$60,000
Virginia Tech	10	\$582,397
Total	11	\$642,397

Figure 2.7: FY26 - SWVA Node Cybersecurity Research Program.

Title of the Research Program

FY26 Research Engagement Program. The FY26 Research Engagement Program provided seed funding to support projects focusing on pilot demonstrations for research programs or funding student researchers for cybersecurity research experience.

Objective of the Call

The Commonwealth Cyber Initiative (CCI) is establishing Virginia as a global center of excellence at the intersection of security, autonomous systems, and data. With a mission of research, innovation, and work-force development, CCI serves as a catalyst for the commonwealth's long-term leadership in this sector through the collaboration of a statewide hub and four regional nodes. The SWVA Node is offering this Research Engagement Program (REP) to seed research pilots, proof-of-concept demonstrations, and student researcher support during Summer 2026. Research Aims: Proposals will be considered seeking to explore early-stage pilots and proof-of-concept demonstrations for cybersecurity-related capabilities, concepts, or programs. Focus areas should address pressing issues related to the intersection of data, autonomy, and security. Ideal outcomes for this seed grant would be A) validating the commercial or theoretical basis for a new cybersecurity-related capability or program, B) pursuing and securing additional, non-CCI funding in future fiscal years, or C) supporting and reporting on cybersecurity-related research efforts available to undergraduate or graduate students over the summer.

Selection Criteria

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

Intellectual merit (40%)

- 1. Clearly defined problem or need within cybersecurity
- 2. Demonstrate theoretical or preliminary approaches and results
- 3. Highlight potential impact of likely or realistic outcomes

Impact of Funding (30%)

- 1. Demonstrate the need for funding to pursue your goals
- 2. Highlight the approach to secure future, non-CCI funding
- 3. Showcase how the funding will impact student or junior faculty research careers, if applicable

Alignment and Qualifications (30%)

- 1. Highlight relevance to CCI mission and suitability of team background to proposed work
- 2. Special consideration is given to first-time CCI researchers and faculty who have not received CCI support in the past 3 years

Research Grants Awarded: 12

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
Radford University	2	\$30,000
Virginia Tech	10	\$149,999
Total	12	\$179,999

Figure 2.8: FY26 - SWVA Node Research Engagement Program

Additional SWVA Node Research Awards

CCI SWVA issues funding strategically to support major initiatives, high-impact research programming, and to facilitate collaboration with regional industry and partner organizations. The Security Scholars Program is designed to address the need for cost share from faculty members or institutions in pursuit of large extramural awards. This type of commitment is usually funding for a graduate research assistant for the entirety of the research project. CCI SWVA funded 3 security scholars awards in FY26, 2 fulfilling obligations established in Fiscal Year 2025 (FY25) and 1 new award to Dr. Hoda Eldardiry for her proposal “Task Based Model Selection.” Workshop Travel Grants facilitate collaborations across SWVA and beyond to promote Virginia as a global leader in cybersecurity. In FY26, CCI SWVA supported workshop attendance at its first Cybersecurity Researcher Workshop in Arlington, VA, to lay the foundation for future external stakeholders’ meetings with research sponsors, and an international Collaboration Workshop in Ria San Vitale, Switzerland, to promote scholarly activity in coding theory and cryptography. The Researcher Workshop engaged 20-30 researchers via presentations on state-of-the-art cybersecurity topics and related research questions. The 2026 Collaboration Workshop included 30 researchers from 10 countries and concluded with a special edition post-quantum cryptography event called Swissogeny Day, hosted in collaboration with IBM Zurich researchers.

Research Grants Awarded: 18

The number and value of grants are listed in Figure 2.9. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
CCI Engagement	1	\$50,000
Security Scholars	3	\$148,505
Workshop Travel Grants	14	\$13,522
Total	18	\$212,027

Figure 2.9: FY26 - SWVA Node Additional Research Programs

2.2.6 CoVA Node

Title of Research Program

Agentic AI Cybersecurity and Security for Agentic AI.

This call for proposals asked researchers to submit proposals that advance the state of the art of agentic artificial intelligence (AI) for cybersecurity and security for Agentic AI systems. Agentic AI refers to autonomous AI systems that can act independently to achieve goals. The core concept of agentic AI is the use of AI agents to perform automated tasks with limited human intervention. These systems plan, execute, and adapt to complex, multi-step tasks without continuous oversight by using a combination of large language models, reasoning, and action-taking capabilities.

Objective of the Call

- To produce seminal contributions to address agentic AI for cybersecurity and security of agentic AI systems, 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 cybersecurity.

Research Grants Awarded: 6

The number and value of the grants are listed in Figure 2.10. Individual grants are listed in Appendix 3.

University	Number of Grants	Grant Total
Old Dominion	5	\$399,926
William & Mary	1	\$80,000
Total	6	\$479,926

Figure 2.10: FY26 - CoVA Node Agentic AI Cybersecurity and Security for Agentic AI Research Program

2.2.7 CCI Fellows Program 2026

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 FY26 CCI Fellows are pictured in Figures 2-11 through 2-13. They join six Fellows funded in FY23, three in FY24, and two in FY25.

Dr. Daniel Takabi, from ODU, is a FY26 CCI fellow who leads a proposal titled, "Center of Excellence in Artificial Intelligence (AI) Security and Safety." This project will support coordination and proposal writing to develop a proposal to establish a Center of Excellence in Artificial Intelligence (AI) Security and Safety at ODU. The proposed Center will bring researchers from several ODU units together and will enable new advancements in the areas of AI security, privacy, and safety by developing scientific foundations and technological breakthroughs needed to shape the ongoing AI revolution, and pragmatic cross-cutting

methods to deliver adaptive capabilities for the Hampton Roads area, Commonwealth of Virginia, and the nation.

Dr. Jacek Kibilda, from VT, is a FY26 CCI fellow leading a proposal titled, "O-RAN-Compatible Software Radio for Secure and Resilient Mid-to-High-Frequency Spectrum Operation." The U.S. leadership in wireless communications is critical to maintaining economic and national security and to shaping the global evolution of mobile networks towards 6G. In support of this goal, there is a strong and growing interest in open and software-defined architectures for future wireless networks. For instance, the National Telecommunications and Information Administration (NTIA) is awarding \$1.5 billion for accelerating the development, testing, and deployment of O-RAN. Moreover, the Office of the Under Secretary of Defense (OUSD) and the National Spectrum Consortium recently launched an initiative to develop an open-source 5G/6G software stack. While of national interest, these efforts mainly focus on technologies operating in sub-6 GHz operation. However, many of the disruptive innovations in wireless communications, sensing, resilience, and security operate in mid- and high-frequency spectrum bands, i.e., 7-15 GHz and above 24 GHz. The challenge is that software stacks and their orchestration solutions cannot be readily used for mid- and high-frequency spectrum bands, as they lack the capabilities to control phased antenna arrays and reflective surfaces needed to create and steer highly directional beams to ensure coverage and service availability. This project envisions creating a new software-radio platform for simplifying and accelerating experimental research in mid- and high-frequency spectrum for future wireless networks and 6G.

Dr. Sam Noh, from VT, is a FY26 CCI Fellow leading a proposal titled, "Intelligent and Secure Agricultural Systems: A Cyber-Physical-Social Approach to Precision Farming." His project aims to develop intelligent and secure agricultural technologies through a cyber-physical-social systems (CPSS) approach tailored for real-world farming environments. He proposes a suite of innovations that integrate artificial intelligence, solar-powered sensors, microrobotics, and edge-cloud collaboration to address critical challenges in animal health, pest detection, and crop management. Our research focuses on energy-efficient, privacy-preserving, and adaptive AI systems that operate under resource-constrained, dynamic farm conditions. The project will explore behavior-based animal disease detection, drone-coordinated microrobotic pest surveillance, and smart pest management systems powered by solar sensors. This CCI Fellows award will catalyze competitive submissions to NSF CPS Frontiers, DoE ASCR, and NSF GCR programs. The effort bridges expertise from VT and Virginia State University (VSU) and actively engages historically underrepresented communities in agriculture and technology. Our systems emphasize resilience, scalability, and real-world deployability while aligning with CCI's mission in secure cyber-physical systems, autonomy, and data privacy. The project also supports economic development through the potential commercialization of intelligent sensing platforms and regional partnerships with Cooperative Extension networks. By advancing responsible AI and workforce training in cybersecurity and smart agriculture, this initiative will position Virginia as a leader in sustainable, secure, and inclusive agri-tech innovation.



Figure 2.11: Dr. Daniel Takabi



Figure 2.12: Dr. Jacek Kibilda



Figure 2.13: Dr. Sam Noh

2.3 Faculty Recruited

2.3.1 Hub Faculty

The CCI Hub hired one post-doctoral researcher in FY26:

Dr. Sayanta Seth: Dr. Seth’s research focuses on designing intelligent, secure, and interoperable NextG wireless systems that integrate artificial intelligence, digital twins, and open network architectures. His work spans O-RAN, AI-driven spectrum coexistence, cyber-physical systems modeling, and lunar communications, with an emphasis on building deployable, experimentally validated solutions. His research combines high-fidelity simulation, software-defined radio testbeds, and AI-enabled decision-making to address emerging challenges in 6G networks, including spectrum sharing, network automation, and resilient communication infrastructure. He has extensive experience developing O-RAN compliant systems using OCUDU, Open Air Interface (OAI), and near-real-time and non-real-time RAN Intelligent Controllers (RICs).

2.3.2 Node Faculty

2.3.3 SWVA Virginia Node

Dr. Shengwei An; Assistant Professor: Shengwei An is an Assistant Professor in the Department of Computer Science and core faculty at the Sanghani Center for Artificial Intelligence and Data Analytics at VT. His research focuses on the security and privacy of artificial intelligence (AI) systems, spanning both traditional and generative AI models. His interests include adversarial examples, backdoors, model inversion



Figure 2.14: Dr. Sayanta Seth

and membership inference attacks, and intellectual property protection. He has published in top-tier venues such as IEEE S&P, USENIX Security, NDSS, CVPR, and AAAI. An received his Ph.D. in Computer Science from Purdue University.

Dr. Shannon Beck; Director, Virginia Cyber Range: Shannon Beck is the Director of the Virginia and U.S. Cyber Ranges at VT. She brings experience in cybersecurity education, outreach, and research from her previous roles as an Associate Professor in the Computer and Cyber Sciences department at the United States Air Force Academy, the Program Coordinator for the Secure and Trustworthy Cyberspace (SaTC) program at the National Science Foundation, and as a scientist and member of the cybersecurity incident response team at Los Alamos National Laboratory. She holds a Ph.D. in Computer Science from Kent State University.

Dr. Jesse Harden; Assistant Professor: Jesse Harden is an Assistant Professor in the School of Computing and Information Sciences at Radford University. Dr. Harden attended Tidewater Community College before transferring to Radford to complete a Bachelor's Degree in Mathematics, followed by two Master's Degrees in Statistics and Data and Information Management from Radford University's Data and Information Management (DAIM) program. Dr. Harden received a Ph.D. in Computer Science from VT before returning to join the faculty at Radford. His research interests focus on large, high-resolution displays and their use in and benefits for data science.

Dr. Rodrigo San Jose Rubio, Presidential Postdoctoral Associate: Dr. San José Rubio's research focuses on algebraic coding theory and its applications to cryptography and quantum error-correction, using techniques from commutative algebra and algebraic geometry to design codes suited for these applications. Before joining VT, he was a postdoctoral researcher at the University of Valladolid in Spain, where he also earned his Ph.D., Master's degree, and undergraduate degrees in Mathematics and Physics. He was drawn to VT by its Applied Algebra Research Group, one of the leading coding theory groups in the United States, and by existing collaborations with his mentor Hiram H. López and faculty members Gretchen L. Matthews and Eduardo Camps-Moreno.

Dr. Emily Van Milligan, Presidential Postdoctoral Associate: Dr. Van Milligen was awarded the Presidential Postdoctoral Fellowship in summer 2025 and works in the VT Center for Quantum Information Science and Engineering (VTQ) with Professors Sophia Economou, Ed Barnes, and Sumeet Khatri. Her research centers on distributing entanglement over quantum networks for sensing applications. She received her Ph.D. in Physics in 2025 from the University of Arizona and her B.S. in Mathematics and Physics, summa cum laude, from Tufts University in 2018.

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 FY26, CCI's xG testbed has inaugurated its outdoor deployment in Blacksburg, VA, currently with two base stations covering an approximately one-mile corridor. The outdoor component of the testbed



(a) Dr. Shengwei An



(b) Dr. Shannon Beck



(c) Dr. Jesse Hardin



(d) Dr. Rodrigo San Jose Rubio



(e) Dr. Emily Van Milligen

Figure 2.15: SWVA Node New Faculty

complements its indoor deployment (in Arlington, VA), allowing researchers to test new technologies under realistic deployment conditions. This has already attracted research funding from industry to conduct field tests of technologies expected to be adopted in 6G.

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 2.16 shows the logo developed for the testbed.



Figure 2.16: 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

The **Research Paper Showcase** highlights the impact of CCI’s research investments through 22 peer-reviewed publications featured in leading journals and conference proceedings. Together, these publications advance knowledge and practical solutions across some of cybersecurity’s most pressing challenges, from artificial intelligence and privacy to cyber defense and emerging technologies.

The papers represent collaborations among researchers from Mason, ODU, UVA, Virginia Military Institute (VMI), VT, and W&M, industry partners, and institutions across the United States and around the world. Organized by cybersecurity focus area, the showcase offers a snapshot of the discoveries and innovations emerging from the CCI research community.

Learn more about the Research Paper Showcase on our website.

AI and Autonomous Systems Security Research focused on AI, machine learning, LLMs, federated learning, AI-assisted security, AI benchmarking, and security of autonomous systems.

BOCLOAK: Optimal Transport-Guided Adversarial Attacks on Graph Neural Network-Based Bot Detection Tests the resilience of AI-powered bot detection systems against evasion attacks.



Figure 2.17: We showcase on our website some of the major findings and innovation produced by our researchers in FY26.

Comprehensive Assessment Tool for Prompt Injection Attacks in Large Language Models (LLMs) Evaluates how vulnerable AI chatbots are to prompt injection attacks.

An Empirical Study of LLM Serving in Confidential GPUs Examines the security and performance tradeoffs of confidential AI computing.

FedHusky: Accelerating Hybrid Federated Learning with Client Hopping Improves the efficiency of privacy-preserving distributed AI systems.

MoltGraph: A Longitudinal Temporal Graph Dataset of Moltbook for Coordinated-Agent Detection Provides a dataset for studying coordinated activity by AI agents on social platforms.

OmniVul: A Holistic, Multi-Turn Conversational Benchmark for LLM-Based Vulnerability Assessment Evaluates whether AI models can reliably identify software vulnerabilities.

StealthInk: A Multi-bit and Stealthy Watermark for Large Language Models Enables tracing of AI-generated content through embedded digital watermarks.

Towards AI-Driven Human-Machine Co-Teaming for Adaptive and Agile Cyber Security Operation Centers Explores how AI can improve cybersecurity operations center performance.

Cryptography, Privacy Data Protection Research focused on encryption, post-quantum cryptography, privacy-preserving computation, data anonymization, and privacy/fairness interactions.

Auditing Fairness-Privacy Trade-offs: Subpopulation-Level Effects of Fairness-Enhancing Algorithms Examines privacy risks associated with fairness-enhancing AI techniques.

AXIOS: Energy-Efficient Acceleration of Hash-Based Post-Quantum Cryptographic Schemes on Embedded Spatial Architectures Advances quantum-resistant encryption for resource-constrained devices.

Exposing Privacy Risks in Anonymizing Clinical Data Reveals privacy risks in commonly used data anonymization methods.

FROST: Efficient Single-Round Obfuscation of Search and Result Patterns in Searchable Encryption Strengthens privacy protections for encrypted cloud searches.

SHAFI: Securing Hash-Based Post-Quantum Cryptography from Hardware Fault Injection Attacks Protects next-generation encryption against hardware-based attacks.

THENA: Accelerating Torus Fully Homomorphic Encryption on Energy-Efficient Heterogeneous Architecture Accelerates computation on encrypted data while reducing energy use.

Cyber Defense and Threat Detection Research focused on attack detection, incident response, cyber operations, threat hunting, evasion, provenance analysis, and intrusion detection.

Catch Me If You Can: Detector-Resistant Evasion via Semantics-Preserving Command Re-Realization Demonstrates how attackers can evade current security detection tools.

LIPPEN: A Lightweight In-Place Pointer Encryption Architecture for Pointer Integrity Protects software from memory-based attacks with minimal performance impact.

Neurosymbolic Learning for Advanced Persistent Threat Detection under Extreme Class Imbalance Combines AI and logical reasoning to detect advanced cyberattacks.

Provexa: Enabling Efficient Attack Investigation via Human-in-the-Loop Security Analysis Helps analysts investigate complex cyberattacks more efficiently.

Extended Reality Emerging Platforms Research focused on emerging computing environments, immersive technologies, XR/AR/VR, and novel platform security challenges.

EyeSpy: Inferring Eye Gaze via Side-Channel Attacks Against Foveated Rendering Identifies a new privacy threat affecting virtual reality systems.

Rethinking Privacy Indicators in Extended Reality: Multimodal Design for Situationally Impaired Bystanders Improves privacy notifications for bystanders in augmented reality environments.

Visceral Notices and Privacy Mechanisms for Eye Tracking in Augmented Reality Helps users better understand and manage eye-tracking privacy risks.

Human-Centered Cybersecurity Research focused on cybersecurity awareness, behavior, education, usability, and human factors.

Interactive Theatre as an Andragogical Tool: Assessing a Cybersecurity Program Across Adult Age Groups Evaluates interactive theater as a tool for cybersecurity awareness education.

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 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 20-21, 2026. 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. TechDuels 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. 142 students from 18 colleges and universities competed over the weekend. Friday's activities included a keynote speech by Pat McShea, Executive Director, CACI/Cyber Mission Operations, and the TechDuels competition. The winners of the capture-the-flag-style Virginia Cyber Cup competition for the four-year college division are: Mason in first place, UVA in second place, and W&M in third place. For the community college division: Germanna Community College in first place, Danville Community College in second place, and Tidewater Community College in third place.

3.1.2 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 FY26, CCI partnered with four industry partners and supported 16 students. CACI continued its commitment to Virginia students by hosting three students during a CACI work-study program. GuidePoint Security hosted five students for a SOC-in-the-Box program. The Public Broadcasting System hosted four students to develop a Data Privacy Program for PBS. LMI hosted four students to perform IoT Protocol Testing, Benchmarking, and NIST Standards Compliance Roadmapping.

3.1.3 Clearance Preparedness Program

In FY26, the CCI Hub continued a virtual series to prepare students for the security clearance process, after three successful cohorts in FY23, FY24, and FY25 with over 500 students registering. This program, entitled "The Clearance Preparedness Program," includes six 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 all 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. The FY26 cohort had 188 students attend some or all of the sessions, with 75 students attending all sessions and receiving a digital badge.

3.1.4 Experiential Learning Program in FY26

The Experiential Learning Program is CCI’s longest-running program. In its seventh iteration, the 2026 Experiential Learning call for proposals elicited 32 submissions, with eleven successful proposals totaling \$1,091,262 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 projects funded by this program are summarized below.

- Securing the Skies: A Drone-Centric Cybersecurity and AI Experiential Learning Program:** Dr. Sherif Abdelhamid, VMI. The rapid adoption of unmanned aerial systems (UAS) across sectors such as agriculture, infrastructure, and emergency response has introduced new cybersecurity challenges within cyber-physical environments. However, current cybersecurity education often lacks hands-on experience with autonomous systems. “Securing the Skies: A Drone-Centric Cybersecurity and AI Experiential Learning Program” addresses this gap through an applied, student-centered training model integrating drone engineering, cybersecurity, and artificial intelligence. Students from VMI, VT, VCU, and Mason will participate in a multi-phase program that begins with building and configuring drone systems, followed by engagement in Drone Capture-the-Flag (CTF) and racing challenges that simulate adversarial environments. In the final phase, students develop AI-based drone detection and classification systems using multimodal data to support anti-drone operations and critical infrastructure protection. The program culminates in a statewide Drone CyberOps Hackathon and Competition, where teams are evaluated on racing performance, cyber defense, attack strategies, and AI detection models. Industry partners, including iVUE Robotics, Xelevate, and Agricism Inc., provide real-world scenarios, mentorship, and evaluation. Program outcomes will be assessed using performance-based metrics such as system functionality, challenge completion, competition results, and model accuracy. This project advances experiential learning and workforce development by preparing students with practical skills in cybersecurity and autonomous systems, aligning with the goals of the CCI.
- Preparing the Incoming Cybersecurity Workforce Through the Professional Readiness Experiential Program (PREP):** Dr. Brian Ngac, Mason. This proposal seeks \$100,000 in funding to scale and enhance Mason’s Professional Readiness Experiential Program (PREP) to prepare students for the cybersecurity workforce. Through partnerships with industry participants such as FWI, the Institute for Defense Analyses, Maximus, Mobius, and the United States Cyber Command, PREP will provide 20 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 CCI’s 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 \$60,300 further underscore their point of view of the program’s importance and impact.
- From Signals to Action: Experiential Learning for AI-Enabled Critical Infrastructure Security:** Dr. Jundong Li, UVA. Virginia’s power utilities, water authorities, and their cybersecurity partners increasingly rely on AI-enabled monitoring and decision-support. A gap is already visible: recent graduates can read an AI alert without knowing what to do with it. Closing that gap takes supervised practice on systems that behave like real critical infrastructure (CI), not classroom

demonstrations or static case studies. From Signals to Action is a 12-month experiential learning program that provides exactly that practice. At the UVA, W&M, and Piedmont Virginia Community College (PVCC), 60–80 students move through three stages: guided fall modules that teach them to turn AI outputs into operational decisions, a cross-institution spring red-team/blue-team competition, and summer placements with regional utility and water-authority collaborators and the UVA Link Lab. Students work inside two open-source CI simulators—one for power grids, one for water distribution—and build a graded portfolio (attack-attribution reports, trust-calibration memos, a cross-thrust capstone) mapped to the NICE (National Initiative for Cybersecurity Education) Workforce Framework competencies. The program is designed for access, not only depth: a funded consultant at PVCC anchors a two-year-to-four-year transfer pathway so community-college students enter on equal footing with peers at the two flagship institutions. Additionally, a senior research-science advisor from Peraton Labs—a Virginia-based firm developing cybersecurity and AI solutions across defense, energy, finance, and communications—will serve as an unpaid industry collaborator, providing feedback on the program’s alignment with industry practice and engaging directly with students on the UVA campus. All modules, rubrics, and scenarios are released under permissive licenses, so any CCI partner can adopt them without additional infrastructure investment. The outcome is a workforce that can act on, not merely observe, the AI signals that increasingly mediate Virginia’s critical-infrastructure defense.

- Immersive Cyber Range for Workforce Readiness: AI-Driven XR Training Across Virginia’s Critical Infrastructure:** Dr. Aesalan Heydarian, UVA. This project establishes Virginia’s first immersive cyber range that combines multi-agent LLM-driven adversaries, VR/XR environments, and hardware-in-the-loop integration to train students for operational technology cybersecurity roles. Three scenarios, spanning pharmaceutical manufacturing, research-computing data center, and transportation signal control, place students inside realistic incident-response situations where AI-driven adversaries adapt in real time to trainee decisions, while the immersive frontend captures fine-grained behavioral data for performance assessment. Hosted in UVA’s Link Lab, the program engages 60+ students across three or more CCI institutions through an experiential-learning pipeline spanning twelve months. Six co-paid summer 2027 interns lead scenario and LLM-agent development. Two UVA undergraduate research assistants support year-round lab operations. Twenty-plus students engage through UVA’s Spring 2027 VR/XR course, taught with a Leidos senior engineer. Two multi-institution workshops aligned with Link Lab industry days connect students to Leidos, Azbil, Elder Research, and other employers. Up to ten Charlottesville High School students participate in a Link Lab mentored capstone. Industry engagement anchors every program activity. Leidos, a senior OT cybersecurity manager at a Virginia-adjacent medical-device manufacturer, VDOT/VTRC engineers, and additional Link Lab affiliates provide mentorship, scenario review, and hiring pathways. The project addresses Virginia’s most acute cybersecurity workforce gap by training students directly for OT Cybersecurity Engineering roles while building fluency in AI, VR/XR, and human-AI interaction, the converging technical skills reshaping the field.
- CyberBridge Fellows: A Multi-Institution Experiential Learning and Internship Program for Cybersecurity Workforce Development:** Dr. Abhishek Phadke, Christopher Newport University (CNU). The CyberBridge Fellows program is a multi-institution experiential learning initiative that connects undergraduate students from CNU, W&M, and ODU with prospective employers for cybersecurity training and career opportunities. In partnership with the Neptune Shield (NS) Foundation, a nonprofit cybersecurity and innovation organization based in Virginia Beach, the program provides students with hands-on exposure to cybersecurity operations and tools, as well as career preparation. The program operates in two phases over a 13-month performance period. In Phase 1, students participate in workshops, lab exercises, and cross-campus activities, including a skill swap session, a capture-the-flag competition, and a hackathon. Training topics span incident response, penetration testing, security operations, and compliance frameworks. In Phase 2, students complete an internship at Neptune Shield, working alongside cybersecurity professionals on active projects and gaining direct exposure to business operations in the defense and maritime cybersecurity sectors. Thirty students, selected through a coordinated selection process, will participate as a named cohort, the CyberBridge Fellows, drawn from cybersecurity programs at all three institutions. Students are compensated through stipends for the full 80 hours of program participation. Each Fellow produces a

deliverable presented at their home institution’s capstone fair or research symposium. The program advances CCI’s workforce development mission by providing students across the commonwealth with sustained engagement with a real-world cybersecurity organization and preparing them to enter the cyber workforce upon graduation. Student performance, satisfaction, knowledge progress, and post-cohort employment data will be collected, evaluated, and used as a key metric for cohort success at the end of the program.

- **Cyber Ready: Experiential Workforce Development for Community College Learners:** Chris Carter, Director, Virginia Space Grant Consortium. Empowering individuals through experiential learning is a vital catalyst for economic growth and workforce satisfaction. The Virginia Space Grant Consortium (VSGC), a CoVA team member, proposes “Cyber Ready: Experiential Workforce Development for Community College Learners.” This project will place Virginia community college students in paid work-based experiences, supporting CCI Goal 2 to close the cybersecurity workforce gap. Community college students from two distinct regions and industry partners from across Virginia will participate in skills-based cybersecurity industry workforce experiences that build both technical and professional skills.
- **Experiential Learning Program for AI-Driven Cybersecurity of RF and Edge-Enabled IoT Systems;** Dr. Dimitrie Popescu, ODU. This project develops a multi-institution experiential learning program to train students in AI-driven cybersecurity for RF and edge-enabled IoT systems, addressing critical workforce needs in defense and wireless technologies. Students will engage in hands-on projects involving RF signal analysis, machine learning–based classification, adversarial attack modeling (e.g., backdoor injection and signal manipulation), and implementing defense mechanisms in real-world industry-driven scenarios provided by partners, including the U.S. Navy, which is a major employer in Virginia. In particular, the proposed program leverages the existing U.S. Navy Cooperative Research and Development Agreement (NCRADA) established between ODU and Naval Surface Warfare Center Dahlgren Division (NSWCDD) to integrate hands-on training, mentorship from RF engineers and cybersecurity professionals, and collaborative projects to prepare students for careers in the US Navy where expertise in RF signal detection and cybersecurity is required. The project combines technical training, applied research, and industry mentorship to prepare students for careers in cybersecurity, RF systems, and AI-enabled applications. Through collaboration between ODU and VCU, the program promotes cross-institution teamwork and scalable training infrastructure. By providing training on RF systems, artificial intelligence, and cybersecurity, the project contributes to developing a highly skilled workforce aligned with the mission of the CCI and the needs of Virginia’s defense and technology sectors.
- **Building the Healthcare Cybersecurity Workforce:** Dr. Sanchari Das, Mason. We propose a multi-institution experiential learning and workforce-development program in healthcare cybersecurity, a representative high-consequence critical infrastructure sector, to prepare Virginia students for cybersecurity careers in operational environments. Led by Mason in partnership with JMU, the program is supported by NewPush, a cybersecurity company providing access to security platforms and hands-on labs, and by the Center for Infrastructure Security in the Era of AI and its partner ecosystem. The program addresses urgent workforce needs at the intersection of cybersecurity and healthcare, where security failures can disrupt care, expose sensitive data, and create significant operational and patient-safety risks. The program, open to students from all CCI institutions, uses a phased participation model. In the first semester, approximately 100 students will participate in a four-part webinar series introducing healthcare cybersecurity, clinical risk, adversarial thinking, and AI-supported analysis. Through a competitive process, 30 students will advance to an intensive hands-on phase consisting of workshops, mentored team exercises, a healthcare-focused CyberAI hackathon, and an employer-facing showcase. Activities will focus on realistic scenarios involving medical devices, patient portals, and hospital systems, implemented in partnership with NewPush. Students will also work with practitioner mentors to configure these environments, analyze attack paths, and develop practical mitigations. Through the Institute for Digital Innovation, which Co-PI Albanese directs, and its partner ecosystem, the program will incorporate real-world use cases and enable direct interaction with potential employers. Expected outcomes include improved cybersecurity workforce readiness,

reusable training materials, and measurable pathways to internships and employment.

- **ACCEL: AI-native Cyber Experiential Learning for CyberWorkforce Readiness Across Hampton Roads:** Dr. Safdar Bouk, ODU. The AI-native Cyber Experiential Learning (ACCEL) program is a multi-institution experiential learning program led by ODU and CNU to prepare Virginia students for cybersecurity careers. The program integrates AI-assisted cybersecurity workflows, hands-on cyber range exercises, and mentor-guided industry case studies to provide students with authentic experience aligned with modern cyber operations. Students will progress through structured modules in threat detection, incident triage, cyber defense analytics, secure workflow orchestration, and human-in-the-loop use of agentic AI, while working on realistic scenarios informed by employer needs. The technical framework combines controlled cyber range environments, explainable AI-enabled decision support, evidence-based assessment, and portfolio generation mapped to workforce-relevant cybersecurity competencies. ODU will lead technical platform development, cyber range integration, assessment design, and program coordination, while CNU will support student recruitment, technical mentoring, project coordination, and cross-institution participation. SimIS will serve as an employer partner by contributing mentorship, practical cybersecurity use cases, and workforce-facing engagement opportunities. ACCEL is designed to create a scalable regional pathway from classroom preparation to cyber workforce readiness, internships, and employment, while advancing CCI's mission at the intersection of cybersecurity, autonomy, and data.
- **Cannons & Cannoneers: Scaling Virginia's Cyber Talent Pipeline Through Student-Veteran Paired Engineering Teams:** Dr. Laura Freeman, VT. N2O, a Charlottesville-based defense software firm, seeks \$91,300 from CCI to fund the expansion of a student-veteran paired engineering program, placing Virginia computer science students into defense-oriented software roles. Four Cannons, drawn from VT, UVA, and additional CCI institutions, will work alongside veteran engineer mentors ("Cannoneers") on live contracts, including work for the DoD's Chief Digital and Artificial Intelligence Office (CDAO) and internal ontology programming. Every project gives Cannons an immersive, security-first professional experience that classroom instruction cannot replicate. N2O's Spring 2026 recruiting cycle drew 1,300 applications and resulted in 12 offers, all of which were accepted over competing offers from FAANG and quantitative finance firms. No engineer has left N2O since the company was founded in May 2025. VT, through the VT National Security Institute (VTNSI), serves as the lead academic institution and transfer partner to the CDAO AI Accelerator. N2O is the sole employer and industry partner, contributing matching funds through Cannoneer mentorship hours, CCI Symposium travel, and above-threshold student wages. The program directly advances CCI's workforce development mission and Virginia's Top State for Talent agenda by retaining high-caliber cyber talent inside the commonwealth, scaling across multiple CCI member universities, and building a replicable blueprint for sustained pipeline growth in Virginia's defense cyber ecosystem.
- **Securing AI-Driven Healthcare: Experiential Cyber Learning for Next-Gen Nursing Workforce:** Dr. Eyuphan Bulut, VCU. Nurses are central to healthcare delivery and are increasingly interacting with AI-enabled and connected clinical systems. While these technologies improve efficiency and patient care, they also introduce cybersecurity and privacy risks that frontline users are often unprepared to recognize or mitigate. This project develops an experiential learning program that equips nursing students with both AI competency and foundational cybersecurity awareness. The program will be implemented at the VCU School of Nursing, with participation from additional CCI member institutions. It consists of three integrated components: (i) a Smart Healthcare Security Lab providing hands-on exposure to AI-driven medical technologies and their associated risks; (ii) a Nursing Cyber Fellows program offering structured training on AI, data privacy, and cybersecurity; and (iii) short-term externships with healthcare partners such as VCU Health. The project will engage over 100 students through lab activities and train up to 15 Fellows in depth. Expected outcomes include improved awareness of cybersecurity risks, increased confidence in using AI tools safely, and exposure to technology-enabled healthcare careers. This project provides a scalable model for preparing a cyber-aware healthcare workforce in Virginia and establishes a foundation for future expansion.

3.1.5 Cyber As A Service

In Fiscal Year 2024 (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 FY26, we continued this program and awarded three projects involving 13 students. Dr. Aurelia Nicholas-Donald from VSU sponsored "AI-Powered Cybersecurity-as-a-Service (CaaS) Platform for Local Minority Businesses." Mr. John Costanzo from ODU and the CCI CoVA sponsored two programs, "CoVA CCI Cyber Clinic with City of Suffolk," and "Student-run Security Operations Center (SOC)" on the ODU Campus.

3.2 Node-led Programs

In addition to the CCI-wide programs described above, the CCI Nodes also developed and executed many successful workforce programs over the past year.

3.2.1 NoVA Node

To meet the continuously expanding demand for cybersecurity talent, CCI's NoVA Node is developing new talent pools to expand the pipeline of cybersecurity expertise, in addition to and beyond those seeking degrees in cybersecurity, computer science, computer engineering, software engineering, information technology, and related majors. CCI's NoVA Node is developing programs to target earlier in the pipeline, such as K-12, and in new sectors for tech talent, including career changers and those not yet skilled in typical cybersecurity-related skills. Experiential Learning, such as internships, research assistantships, and apprenticeships, remains one of the most effective mechanisms for developing real-world cybersecurity skills. CCI NoVA Node has made significant investments in workforce expansion by developing and funding experiential learning opportunities that not only broaden the range of skills but also 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 five (5) workforce initiatives during FY26.

- **High School Cybersecurity Internship Program:** CCI NoVA Node has scaled this program to support 50 high school students for internships with cybersecurity companies during Summer 2026. The experience includes a 2-week professional skills training program to prepare students for the professional work environment. 224 applications were received for the 50 available placements. Of the selected applicants, 20% identify as women and 36% come from underrepresented populations in science and engineering. Additionally, 20% of participants will be the first in their families to attend college. Host companies include: Appian, CGI Federal, Chainbridge Solutions, Deltek, F1 Cloud Solutions, GT Edge AI, Leidos, Maximus, NT Concepts, Obscurity Labs, Oceus Networks, Pingwind, SES, SixGen, Solvitur Systems, Tyrula LLC, Unissant, and VT's Thinkabit Lab. This program is an expansion of the successful program launched in FY21 and scaled in FY22, FY24, and FY25.
- **Undergraduate Research Program** CCI's NoVA Node sponsored 66 undergraduate students conducting cybersecurity research at Mason, JMU, and University of Mary Washington (UMW). 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. Seventeen percent (17%) of this year’s Undergraduate Research Assistants cohort identify as women, and 23% 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 provides 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 8, 2026, followed by a 12-week apprenticeship/traineeship with a cybersecurity company. The program received over 150 applications for 19 available positions. Thirty-seven percent (37%) of the cohort identify as female. Underrepresented population groups in science and engineering comprise 63% of this cohort. Placement in apprenticeships is ongoing, and hosts include, to date, Peraton and Solvitur Systems
- **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 37 students participating in this program, with more onboarding. Industry hosts include 9th Way Insignia, Auspex Labs, Blue Sky Innovators, Critical Shift Corporation, EngineerRD, Great Victory Legends, Summit Knowledge Solutions, SyncData AI, Rapid Prototyping Research Center, and TekScope. Thirty-three percent (33%) of this cohort identify as female, and 54% identify with underrepresented population groups in science and engineering.
- **Cybersecurity Field Training Experience (C-FTE)** As part of CCI NoVA Node’s effort to strengthen the cybersecurity workforce through experiential learning, the CCI NoVA Node piloted the Cybersecurity Faculty-Training Experience (C-FTE) program, pairing graduate student subject matter experts and project supervisors with undergraduate students to complete cybersecurity projects in collaboration with industry and government partners. Graduate students served as technical mentors, sharing their expertise while guiding undergraduate team members through project activities and developing the leadership skills expected of early-career technical managers. The pilot also expanded access to cybersecurity by engaging undergraduate students from disciplines beyond traditional cybersecurity programs, including information technology, mathematics, and business, providing opportunities to develop technical cybersecurity knowledge and skills through applied project experience. Through this model, undergraduate students gained hands-on experience that prepared them for entry-level cybersecurity careers, while graduate students strengthened their technical leadership and project management capabilities. Twenty-seven percent (27%) of this cohort identify as female, and 47% identify with underrepresented population groups in science and engineering. Participating hosts included Naval Surface Warfare Center – Dahlgren, the Rapid Prototyping Research Center, and JSI (<https://www.jsitelecom.com/>).

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. NoVA Node supported CyberSlam 2026, which brought together members of the Secret Service, Homeland Security, high school teachers, Mason faculty, and more than 600 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 2026, which attracted over 500 students to develop their technical capacity to address real-world problems presented by industry, as well as Hack TJ, which attracted over 400 high school students from across the region. Additionally, CCI NoVA Node sponsored summer programming at UMW, exposing 10 students to cybersecurity. Finally, in 2026, NoVA Node launched the inaugural season of its Cybersecurity Drone League, a competitive event bringing together 35 students representing seven (7) teams from Mason, JMU, and

Northern Virginia Community College (NVCC). These programs supported short cybersecurity experiences for 1545 students.

Given the longevity of CCI NoVA Node, we now have sufficient historical data to evaluate long-term workforce outcomes across our programming. Since fiscal year 2022, CCI NoVA Node has increased its participant retention rate in the cybersecurity arena after participation in its workforce development programs (defined as either obtaining full-time employment or pursuing further education in cybersecurity or a closely aligned field), rising from 86% in FY22 to 97% in FY25.

3.2.2 CoVA CCI

- **Innovate Cyber Challenge.** CoVA CCI completed another cohort of its Innovate Cyber Challenge in spring 2026 with a total of 41 students from eleven (11) universities and colleges. These included CNU, Mason, J. Sargent Reynolds Community College, NVCC, ODU, Tidewater Community College, Virginia Peninsula Community College, UMW, UVA, VT, and W&M. This program groups students into teams, and each team is assigned a cybersecurity problem/challenge. Over the semester, the teams use design thinking to develop unique solutions to the problem and present their final products at a Showcase event in April 2026. This year's challenge asked: How might we design humane, transparent, and trustworthy cybersecurity experiences that empower everyday people to understand, control, and ethically participate in protecting their digital lives? The teams participating in this year's cohort are:
 - Cyber Bridge VR
 - Click Smart
 - Trace
 - UpdateRadar
 - Breachwatch
 - ClearAgree
 - Vigil
 - ClearShield
 - SafeEarn
 - Vault 07
- **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. ODU, 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 909 students completed an internship experience.
- **Internships with CEIO:** CoVA CCI supported thirteen (13) interns for ODU's Center for Educational Innovation and Opportunity (CEIO). These students assisted CEIO by engaging with the diverse programming offered at CEIO 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 CEIO organizational tasks, including maintaining equipment, supporting program planning, and creating marketing materials. Their involvement included collaborating with community partners and providing valuable administrative assistance, enabling 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.
- **CoVA CCI Cybersecurity Clinic:** Starting with a pilot cohort in the Spring 2024 semester, CoVA CCI supported a Cybersecurity Clinic with eight (8) students from ODU, 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 businesses. This program has continued to expand each semester. Since its inception, the cyber clinic has supported 83 students and 25 local businesses. This clinic offers free cybersecurity-as-a-service to small businesses, non-profits, local government offices, agencies, boards, and other organizations. Selected students evaluate these organizations' cybersecurity readiness and risk posture. The goal of this clinic is to raise cybersecurity awareness and provide services, such as education and risk management strategies, to client organizations within Hampton Roads. It also offers students an opportunity for experiential learning as cybersecurity interns/consultants. Specifically, this clinic targets client organizations that lack a strong cyber presence and can benefit from cybersecurity awareness initiatives and services. This is a 16-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 services to the client in one or more areas of cybersecurity, including network defense, policies and procedures, employee cybersecurity training, 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.

- **Student Security Operations Center (SOC):** With support from the CoVA CCI, the Student SOC provided students with the opportunity to contribute directly to ODU cybersecurity operations, while gaining practical, hands-on experience in a real SOC environment. The students worked alongside UIISO security staff to support daily SOC functions, assist with Tier 1 alert response, and help expand the university's monitoring and response capacity. The SOC serves as the central point for reviewing, triaging, escalating, and responding to cybersecurity alerts across ODU's technological environment. Its purpose is to help identify potential security incidents early, reduce institutional risk, and ensure security events are reviewed and handled consistently. During the internship, student interns provided Tier 1 SOC support on scheduled Student SOC coverage days. Their work included reviewing and triaging security alerts, documenting initial findings, escalating events that required further investigation, and assisting with operational requests. Students also supported the processing of firewall policy changes, giving them exposure to both alert response and security operations workflows. The students reviewed more than 1,000 security alerts and supported approximately 150 firewall change requests during the reporting period. This work provided measurable operational value to the SOC by increasing Tier 1 review capacity and reducing the workload on full-time analysts. With students handling review and routine support tasks, professional SOC staff were able to spend more time on higher-priority investigations, complex incidents, and process improvement. The program also served an important role in workforce development. Students gained practical experience using security tools, following documented procedures, communicating findings, and understanding how alerts move from initial review through escalation and response. This helped prepare students for cybersecurity roles while also demonstrating that a structured Student SOC model can provide real operational benefit to the university.

Overall, CoVA CCI funding supported a student-centered SOC model that strengthened security operations, expanded monitoring and response capabilities, and provided students with valuable applied cybersecurity experience.

3.2.3 SWVA Node

CCI supports workforce development initiatives tailored to the regional needs of SWVA, which has historically embraced industries without a cybersecurity focus, exacerbating the commonwealth's cybersecurity worker shortage. Support largely takes the form of grants for workforce development programming at various institutions of higher learning in the CCI SWVA network, event support for the career preparedness of students considering cybersecurity careers, and internship subsidies to promote in-depth experiential learning for cybersecurity and cybersecurity-adjacent students in the region, in partnership with local businesses and governments. These three categories are designed to address the region-specific needs of communities in

SWVA while promoting SWVA and Virginia as viable destinations for the cybersecurity industry.

Workforce Grants from Appropriated Funds In FY26, CCI SWVA awarded 3 grants to Radford University and 2 awards to VT. Supported efforts were drawn from applications to the FY26 Cybersecurity Research Call for Proposals with strong experiential learning or workforce development potential, or were a continuation of prior programming as reported to Virginia Works. CCI SWVA continued its support for the Professional Accelerated Cyber Education (PACE) Program at Radford University, aimed at strengthening cybersecurity workforce development in SWVA, and highlighted at the 2026 CCI Symposium as the recipient of the prestigious IMPACT Award. Radford University also received a grant comprising travel support for their Experiential Learning: UK Cryptology Trip, designed to engage students in the field. CCI SWVA continues its support of Radford University's RUSecure program, a massive capture-the-flag (CTF) competition that hosts teams of up to 5 students each in a cybersecurity competition that has been streamed on Twitch.tv: 1,084 students participated in the Fall 2025 preparatory round, with 78 teams and roughly 312 student participants advancing to the Spring 2026 final round.

In addition, CCI SWVA continues its support of Dr. Matthews's outreach and workforce development efforts as CCI SWVA Director. The final workforce grant is highlighted below as contributions to the Living Learning Community Securitas. The Securitas Living Learning Community (LLC) offers students an immersive experience centered on cybersecurity, leadership development, and community engagement. The LLC supported 52 undergraduate students in FY26. Through weekly Cyber Monday meetings, academic support, guest speakers, networking opportunities, collaborative events, and social programming, students developed technical knowledge while strengthening communication, teamwork, and leadership skills in a supportive community. Throughout the year, students grew by participating in leadership roles, professional development opportunities, and community-building initiatives. Securitas LLC remained committed to preparing students for future careers by connecting classroom learning with real-world experiences and fostering an inclusive environment where students could succeed academically, professionally, and personally. In partnership with VT's Pamplin College of Business and the VT National Security Institute, CCI SWVA invested in Securitas to support salary and fringe costs for the program director and the academic coordinator, and to support programming and operational budget along with a student intern.

FY26 Workforce Development Events

- **Cybersecurity and the Intelligence Community:** In partnership with the Applied Algebra Research Group and the VT Department of Mathematics, CCI SWVA hosted speakers from the government agencies and the intelligence community for 2 1-hour presentations, followed by a Job and Internship Opportunities Panel.
- **VTQ Hackathon:** In partnership with CCI SWVA, the VT Center for Quantum Information Science and Engineering partnered with IBM Quantum to host a hackathon. Winners received over \$700 in prizes, and all participants received an official IBM Quantum certificate. With the only prerequisite for participants being prior experience with Python, this event was a great opportunity for those who are interested in quantum computing to gain initial exposure and experience.
- **Joint Integrated Security - Applied Algebra Seminar:** Peng Gao (VT, Computer Science) discussed LLM-Powered Cyber Threat Intelligence and Security Operations as supported by his NSF CAREER Award, which seeks to develop holistic foundations for next-generation, AI-driven security operations centers (SOCs) using frontier AI technologies such as large language models (LLMs). This hybrid seminar was held online and in Steger Hall on the VT Campus.
- **CCI SWVA Graduate Student Summit:** To better prepare graduate students for communicating complex cybersecurity ideas from their research projects to potential employers (academic, industry, or government), CCI SWVA supported a Graduate Student Summit. It provides a platform for any graduate student in CCI SWVA to share 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 finalized results are not required for presentation. The students presented their work, and all attendees provided critical feedback. The presentations were also reviewed by subject matter expert

judges. This feedback helps develop the graduate student's presentation skills and positions them to better articulate their research and outcomes. The Summit, held on November 17, 2025, featured 29 presentations spread across 2 sessions.

- **Cybersecurity, Data Analytics, and AI Panel Discussion at UVA-Wise:** In partnership with UVA-Wise's Institute for Applied Data Analytics, CCI SWVA coordinated a panel discussion of academic researchers, industry leads specific to SWVA, and regional economic development agencies in partnership. Moderated by Dr. Ning Zhou from UVA-Wise's Business and Economics Department, the panel discussed the challenges and opportunities of cybersecurity careers tailored to regional needs in the era of emerging AI. Faculty and industry representatives met with several students before and after the discussion, which led to several funded internship placements in Spring and Summer 2026. In addition, business-academic connections forged at this event led to the submission of a multi-million-dollar proposal to the EDA Disaster Supplemental Grant Program titled "Development and Innovation to Propel Advanced Manufacturing (DIPAM)."
- **FutureScapes Exhibit (Securitas LLC):** On the evening of March 2, 2026, students enrolled in the Securitas LLC launched an exhibit in partnership with the University Library entitled "FutureScapes: Curating Quests through Digital Dimensions." Featured in a VT News article, "FutureScapes" is a program for second-year Securitas students at VT to explore ideas and ways of thinking about technology using history, literature, and artifacts. Throughout the semester, students discussed technology in science fiction and fantasy books with invited experts from departments across VT. They also conducted site visits to the University Archives and the XYZ Gallery in Blacksburg, VA. The culmination of their research was the FutureScapes exhibit." (courtesy Arianna Schuler Scott and Hollis Wittman, VT News)
- **DMV Security Workshop:** The DMV Security Workshop returns for the 2025-2026 academic year on March 20, 2026, to unite researchers in computer security and privacy from Washington, D.C., Maryland, and Virginia. CCI SWVA supported this in-person event with a keynote, lightning talks, speed advising, and breakout discussions focused on building collaborations across the DMV community. Registration remained free, thanks to CCI SWVA's support, to help encourage broad participation.
- **Mathcounts Competition:** VT hosted the 2026 Virginia State Mathcounts competition in Blacksburg, VA, on VT's campus, with 81 middle school students, including 11 teams that had advanced through school and chapter competitions to represent their schools and chapters at the state competition. Graduate student Adam Downs represented CCI SWVA and spoke to the participants and supporters on the importance of cybersecurity and his work in cryptography.
- **RBTC IT Security Forum:** CCI SWVA supported an RBTC-led IT-Security Forum CTF (Capture the Flag) competition held at the Christiansburg New River Community College STEM campus. This CTF features tongue-in-cheek "Hollywood-hacker" style mood lighting, pumping electronica background music, food, drinks, and \$1,000 in IT-Professional themed IT-Security prizes. The Jeopardy-style, 3-hour, hands-on hacking CTF itself is loaded with brand-new challenges designed in partnership with the Virginia Cyber Range, ranging from classic cybersecurity categories such as Cryptography, Recon, Reverse Engineering, and cool new Web challenges, as well as "IRL" (in-real-life) challenges including physical RFID/RF sniffing, network/portscan challenges, and more!
- **CCI SWVA Student Researcher Showcase:** In SWVA, 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 1, 2026, is an opportunity for the students to present their ongoing research projects and share their methods and results to date. More than 30 undergraduate and graduate students presented their work on electronic posters in 25 presentations. Awards were given for best poster, crowd favorite, and best technical presentation.
- **VCyS and VT Cyber Club Summit CTF 2026 "Hack the Airport:"** CCI SWVA provided financial support for the nascent SWVA Node of the Virginia Cybersecurity Students (VCyS) organiza-

tion to partner with the VT Cybersecurity Club to host the 2026 Hacking Tournament in partnership with the DOD Senior Military College Cyber Institute (SMCCI), local cybersecurity firm Triple Point Security, and more. The competition ran 24 hours at the VT Data and Decision Sciences Building, spanning the weekend as 4-person teams from multiple universities competed to take home the prize.

- **Hokie for a Day:** CCI SWVA volunteers, supported by Dr. Schuler-Scott and Dr. Matthews, ran a cybersecurity game for 60 5th graders. Students rotated through in small groups, taking turns as the blue and red teams for a cybersecurity challenge. While CCI SWVA's focus was on teaching and communication for its volunteers, the participating elementary school students left with a new appreciation for cybersecurity as a potential career pathway.
- **BluCyber Forum:** CCI SWVA sponsored 3 budding entrepreneurs to attend the venture capital and investor meeting on May 6, 2026 at Capital One Hall in Tysons, VA, for a day built around high-impact networking, actionable insights, and new opportunities across cyber and AI. Students supported by CCI SWVA were selected from the Cyber Innovation Scholars cohort.

FY26 SWVA Node Supported Internships

CCI SWVA promotes workforce development by subsidizing Virginia-based cybersecurity internships that provide students at member institutions with hands-on experience. Given the regional history of SWVA and the indirect paths by which cybersecurity professionals often enter this field in this part of the commonwealth, CCI SWVA provides internship support for both cyber and cyber-adjacent internships with a cybersecurity focus, following feedback from local businesses and regional economic development organizations. **CCI SWVA funded 72 internship positions across 18 organizations in FY26.**

- Aeroprobe (Summer 2026, 1 Intern): Christiansburg, VA-based defense contractor Aeroprobe hired an IT Intern for 3 months with support from CCI SWVA. This role provided experience in a CMMC/NIST SP 800-171-compliant cybersecurity environment, including hardware, server, and software management.
- CGI Federal (Summer 2026, 2 Interns): Building off of successful student engagement at the panel discussion at UVA's College at Wise, CGI Federal hired 2 interns with a focus on a cybersecurity project exploring emerging topics such as AI Security and Governance and Post-Quantum Cryptography readiness, aligned to mission needs within the Federal Civilian Executive Space. The intern produced research, technical artifacts, and recommendations that integrated competencies from both functional and technical perspectives.
- FCC Internship (Fall 2025-Spring 2026, 1 intern): a postdoctoral associate received full funding for a position at the FCC. Despite interruptions caused by government shutdowns, this associate completed the internship and presented findings at the CCI Symposium in Richmond, VA.
- Food City (Spring 2026, 3 interns): Following successful engagement with regional grocery chain Food City in the February panel discussion at UVA-Wise, Food City hired 3 interns into their IT Department. This cybersecurity internship at a non-cybersecurity firm helps demonstrate that cybersecurity is everywhere and that careers in this field can be found in unexpected yet vital components of any industry.
- GCAPS (Fall 2025, 1 intern): The GCAPS intern was able to successfully complete research on proof-of-concept database design, which has the potential to be utilized in further efforts for technology commercialization.
- Hive Systems (Spring 2026, 1 Intern) Expanding from a successful engagement with CCI's CVN node, Hive Systems recruited 1 intern to give hands-on experience in cybersecurity consulting, risk analysis, and strategic decision-making - all while working alongside industry experts. Responsibilities spanned cybersecurity research and writing, shadowing and supporting cybersecurity consulting work, and technical and policy analysis in alignment with the NIST NICE Framework.

- Music Advocacy Project (Spring 2026, 1 Intern): CCI SWVA supported hiring of a student intern for the Music Advocacy Project, a startup company that recently exited the Roanoke Blacksburg Technology Council's RAMP accelerator program. The startup focused on early-stage application development and security, serving a rapidly growing company that meets the needs of regional music venue providers by safely projecting ticket sales using safeguarded proprietary data.
- Node Project Management CCI SWVA Internship (Fall 2025-Spring 2026, 1 intern): This internship involved learning program/project management and research administration for a statewide cybersecurity initiative. The internships included event management, website maintenance, and other administrative tasks for the successful implementation of node programs and events.
- Radford University Nightwatch (Fall 2025-Spring 2026, 3 interns): Radford University hired 3 student analysts as part of the "Nightwatch team," responsible for monitoring and responding to after-hours security alerts as well as performing in-office cybersecurity tasks on a rotating schedule.
- Roanoke City Public Schools (Spring 2026, 1 Intern): The regional cybersecurity workforce in SWVA is not exclusively concentrated in dedicated cybersecurity firms. To meet regional needs, Roanoke City Public Schools hired an intern, with support from CCI SWVA, to provide information technology support, with a dedicated focus on cybersecurity within a municipal government agency.
- Space@VT Intern (Spring 2026, 1 Intern): Building off the success of a Hack-a-Sat competition supported in part by the US Space Force, VT's Center for Space Science and Engineering (Space@VT) sought to scale their program to include a cybersecurity challenge for students with the goal of hacking satellites first in a local hardware testbed before eventually growing to a hacking competition for a satellite parked in Earth orbit.
- Triple Point Security (36 new enrollees split across 3 cohorts [fall, spring, summer]): Triple Point Security brought on 36 new cybersecurity interns as part of our long-standing commitment to workforce development and regional capacity building in SWVA. The internship program expanded to its largest cohort yet, providing students from VT 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.
- Virginia Cyber Range Internships (Year-round, 3 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 intended to sustain our ability to provide new and interesting CTF challenges by employing student interns with CTF experience and the requisite skills.
- VT College of Engineering Security Operations Center (SOC, Spring 2026, 4 interns [3 spring, 1 summer]): Since its inception, the Student SOC has grown from a 2-department pilot into an operational security program supporting 10 College of Engineering departments. Key achievements include expanding from a 2-department pilot to an operational SOC supporting 10 departments, and eliminating 15 externally exposed high-risk services, reducing the college's attack surface and risk of unauthorized access. During the internship, one student earned the CompTIA Security+ certification.
- VT IT Department (Fall 2025-Spring 2026, 3 interns): The VT IT Security Office (ITSO) and Lab (ITSL) provided a unique opportunity for undergraduate and graduate students to gain hands-on experience working with cybersecurity analysts in a format similar to teaching hospitals, where students work under the supervision of security practitioners. Following program participation, one intern enrolled in a computer science graduate program, one secured a full-time position at a cybersecurity firm in NoVA, and one intern was interning with Cyber Audit and will participate in a US Cyber Challenge Camp in July 2026.

- VPT, Inc (Spring 2026, 2 interns): Blacksburg-based business VPT Power took on two interns in a new collaboration with CCI SWVA. This on-site internship in Spring 2026 enabled two interns to identify and respond to security-related incidents and alerts while maintaining compliance with DOD and CMMC Level 2 requirements. One of the interns transitioned to a full-time role upon completion of the internship.
- VT Mentorship & Academic Outreach Programs (Summer 2026, 7 students): 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 for their specific interests. This 10-week research program provides motivated undergraduate students across the nation the opportunity to work with VT 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 CVN Node

Virginia’s cybersecurity workforce gap is the problem CCI was created to address, and it is the area where CVN’s work is most directly visible. The node’s approach is deliberately layered: competitive grants that build training capacity within member institutions, internship placements that place students in working security environments, and short-form credentialing that gives students a marketable qualification in days rather than semesters. Each layer reaches students that the others do not — doctoral researchers, undergraduates seeking first placements, and community college students who benefit most from a credential they can carry immediately into employment.

FY26 saw that structure widen. The node ran five internship programs, one of them newly launched, added a statewide FAA certification pathway, and reached students across the partner network. Taken together, CVN recorded 144 student placements and training participation during the year.

CVN supported 35 internship placements during FY26, held by 33 distinct students: 13 through the CVN Summer Internship Program, 10 through UVA CCI Internships, 5 through Cyber4n6, 4 through Cyber Guardians, and 3 through Cypher-Bridge. Two students held two placements each, as described above. Note that UVA-delivered programs reflect a partial program year, as FY26 UVA allocation funds were released at the start of the 2026 calendar year. A further 73 students were trained through structured programs — 35 through the AWS AI Academy, 24 through CyberDevOps, and 14 through Drone Training and Certification — and 36 participants completed the Digital Forensics Challenge. Including placements and training, CVN recorded 144 student placements and training participation during FY26. Because two students held two placements each, the number of distinct individuals is lower. Industry-recognized credentials were a particular strength of the year: 8 students earned the AWS Certified Cloud Practitioner certification, 24 certificates were awarded through the Digital Forensics Challenge, and 14 students were made eligible for FAA Part 107 certification, with several already certified. That is 32 credentials earned and 14 more within reach from a single reporting year.

Workforce Grants from Appropriated Funds

- **Workforce Training through Testbed Innovation and Machine Learning for RIS-Enabled Wireless Communication:** Dr. Yanxiao Zhao’s project trained students at the intersection of machine learning, wireless communication, and reconfigurable intelligent surfaces (RIS), with the explicit aim of preparing them for the cybersecurity workforce. Students helped build an RIS testbed, gaining practical experience with advanced hardware and signal processing, and developed machine learning approaches for RIS wireless systems. The training produced a substantive technical result. Three doctoral students — two at VCU and one at UVA — designed E2E-CsiNet, a deep learning framework that jointly estimates channel state information and performs feedback for RIS-assisted wireless systems. The framework pairs a denoising super-resolution network that reconstructs full channel state information from partial observations with an encoder-decoder feedback network that uses channel attention and progressive refinement. In simulation across moderate-to-high signal-to-noise regimes, it achieved a normalized mean squared error 2 to 3 dB lower and a peak signal-to-noise ratio 2.5 to 3.5 dB higher than comparable end-to-end baselines, without requiring uplink channel state information as an auxiliary input. The resulting journal article has been submitted to IEEE Transactions on Cognitive

Communications and Networking and is in its second round of revision. Three students were directly supported: Tahmid Tahi and Syed Samiul Alam at VCU, and Zeyu Zhang at UVA, under Dr. Zhao, with Co-PI Dr. Haiying Shen at UVA — making this the node’s clearest example of a workforce award that produces genuine cross-institutional doctoral training. The project team submitted two collaborative NSF proposals during the reporting period, seeking \$250,000 and \$280,000 to VCU, respectively, for work extending the RIS research program. Neither was funded. They are recorded here because they evidence the node’s investment being used to pursue substantially larger federal awards, and are deliberately excluded from the external funding attracted totals in Chapter 2, which count only awards made or pending.

FY26 CVN Supported Internships

- **Cyber4n6:** 5 Students. This industry-focused experiential learning opportunity bolsters students’ skillsets and resumes, producing a highly qualified cyber workforce in the commonwealth. Students work with the Computer Evidence Recovery Section (CERS) at the Virginia State Police office in Richmond, serving as a direct pipeline into the working world of digital forensics and giving students hands-on experience that sets them apart in the technology sector.
- **Cypher-Bridge:** 3 Students. A partnership between the Federal Communications Commission (FCC) and VCU’s College of Engineering, Cypher-Bridge is an immersive research fellowship rather than a conventional summer placement. Fellows are embedded with the FCC’s Office of Engineering and Technology (OET), building applied AI and machine learning tools that directly support federal spectrum policy and enforcement work. In FY26, the fellowship drew students from both VCU and the UVA, and each fellow delivered a working system rather than a study or prototype.
- **CVN Summer Internships:** 13 Students. VCU’s Career Services Department worked with local start-ups and regional employers to secure internship opportunities for CVN students in fields related to cybersecurity, AI, and data. Thirteen students were placed across ten host organizations for a ten-week summer cycle: Deep Run AI Labs, AMC Technology, VCU Information Security, Hive Systems, Spanalytics, IT4Causes, Weinstein Properties, Virginia Farm Bureau, GRTC, and the State Corporation Commission. Placements at organizations with more than 500 employees are subsidized at 25 percent, with the employer covering the balance, extending the program’s reach beyond what a full subsidy would allow.
- **UVA Summer Internships:** 10 Students. Industry-focused experiential internships administered by the UVA Career Center under CVN’s allocation to UVA, supporting applied learning grounded in cybersecurity fundamentals. Students were placed with Booz Allen Hamilton, Archibald Corporation, Skillbit Labs, Hardshell, Venture Central, and IMCI Technologies, on work spanning secure LLM gateways, IoT edge security, robotics firmware and encoder security, AI/ML data security engineering, and cybersecurity test and validation for critical infrastructure monitoring.
- **UVAAWS AI Academy.** 35 Students. Through a partnership with Amazon Web Services, UVA delivered a five-day immersive program that educated and engaged students in cybersecurity-focused career experiences. Participants gained AI and machine learning foundations tailored to cyber challenges, alongside hands-on activities delivered with Booz Allen Hamilton, and closed with an employer exhibition featuring AWS, Amazon, MITRE, Accenture, CapTech, and IMCI.
- **CyberDevOps: hands On DevOps and Cloud Training:** 24 Students. A cross-institutional workforce development program training undergraduates at VCU and VSU in DevOps and cloud computing — skills in high demand across Virginia but thinly covered in traditional computer science curricula. Students prepared for the AWS Certified Cloud Practitioner examination through self-paced study anchored by weekly check-ins, structured peer study groups, and cross-institutional mentoring, with hands-on work in Amazon Web Services. The grant covered study materials and examination fees, and stipends supported sustained participation alongside coursework and employment. Led by Dr. Kostadin Damevski (VCU) with Co-PI Dr. Denise Daniels (VSU).

- **CVN Drone Training and Certification:** 14 Students. A CVN-wide workforce development initiative led by the UVA, providing students with targeted preparation for the Federal Aviation Administration Remote Pilot Airman Certificate (Part 107), the credential required for commercial drone operation, and one that carries Transportation Security Administration vetting. The training was delivered through Piedmont Virginia Community College’s two-day Remote Pilot Airman Program on 4 and 11 April, and was open to students at all CVN institutions. The program was led by Dr. Lu Feng, Associate Professor of Computer Science at UVA, with Kelley Tobler, Link Lab Program Manager.
- **Cyber Guardians - New in FY26:** 4 Students. Cyber Guardians is CVN’s newest internship program, launched in May 2026, and the only new internship pipeline the node established during the reporting year. Hosted within VCU Information Technology under Dan Han, it places students inside an operating enterprise security function — defending a live institutional environment rather than working through a training scenario.

Chapter 4

CCI Innovation

This chapter summarizes the main achievements in FY26 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 FY26, 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. In FY26, the CCI Hub awarded two Tech Transfer grants to two researchers at CNU.

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 NoVA Node

In FY26, CCI NoVA Node invested to expand the number of new cybersecurity solutions in the commercial market by supporting faculty and early-stage companies with wraparound services to promote the successful development of nascent technologies. In FY26, CCI NoVA Node expanded its support for the highly successful Innovation Commercialization Assistance Program (ICAP) by continuing to invest in the cybersecurity accelerator led by Mason and based at its Mason Square Arlington Campus, in the heart of the growing Rosslyn-Ballston Tech Corridor.

Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT) and Academic Support for Cybersecurity Entrepreneurship and Next-Gen Development (ASCEND) Funds

In 2026, CCI continued to support and execute its 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 accelerating the transition of academic research outcomes to

the marketplace. While these initiatives are led by the CCI NoVA Node, they are open to innovators from across the entire Commonwealth of Virginia. The CATAPULT Fund is supporting seven (7) new awards, of \$75,000 each, in FY26. Additionally, CCI expanded its Academic Support for Cybersecurity and Next-Gen Development (ASCEND) Fund, a mechanism designed to help early-stage companies and startups access and partner with academic subject-matter experts to develop and advance solutions to technical problems they've encountered in industry. The ASCEND Fund is supporting an additional six (6) new awards in FY26 of \$75,000. Both funding tracks require recipients to participate in the Commonwealth Cyber Incubator + Accelerator (CCI+A). An investment of \$950,000 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 NSF. During this phase, innovators are preparing for SBIR or CRCF grants to support product development and market testing, but are not yet ready for outside investment. The CATAPULT and ASCEND Funds are helping innovation teams pay for critical resources, personnel, and time to test products and gather initial market feedback, all of which are integral to securing Seed or Angel funding.

CCI+A Program in Support of the CATAPULT and ASCEND Funds

Launched in early 2022 in the new Digital Innovation Pilot facility on Mason'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 was released in January 2026, with proposals due March 2, 2026. Thirteen (13) new companies and faculty partners were notified of their successful selection for CATAPULT and ASCEND funding in April 2026. The following are summaries of the technology innovations fielded by each of the CCI+A Initiative teams:

CATAPULT Fund Supported Innovation

- *Magnetic Shielding for Cyber Secure Magnetic Random-Access Memory* Dr. Jayasimha Atulasimha, VCU. Spin-transfer torque magnetic random-access memory (STT-MRAM) is an emerging memory technology that offers high speed, low power consumption, and nonvolatile data storage, making it attractive for next-generation computing and embedded systems. However, its adoption has been limited by sensitivity to external magnetic fields, which can reduce reliability in real-world operating environments. This project is advancing a novel magnetic shielding technology that improves the resilience of STT-MRAM by controlling how magnetic interference is absorbed and redirected within the shielding structure. By introducing an innovative shield architecture that prevents localized magnetic saturation and reduces flux leakage, the technology provides more consistent protection than conventional shielding approaches while remaining compatible with existing semiconductor packaging. The project will develop prototype-ready designs, validate performance under realistic operating conditions, and work with industry partners to evaluate integration into commercial memory products. Future efforts will focus on technology maturation, customer discovery, and commercialization through state and federal innovation programs to accelerate industry adoption. By addressing a critical reliability challenge for advanced memory systems, the project has the potential to improve the performance and durability of next-generation electronic devices while supporting the commercialization of university-developed intellectual property in the semiconductor sector.
- *RAEMAP-Display: Decentralized Edge Processing for Privacy-First Multi-User Eye Tracking in Digital Signage*; Dr. Sampath Jayarathna, ODU. RAEMAP-Display is an intelligent digital signage

platform that combines real-time, multi-user gaze tracking with edge-based artificial intelligence to measure audience engagement and dynamically optimize displayed content. The technology is built on a breakthrough that enables accurate, calibration-free gaze estimation for multiple users using an inexpensive off-the-shelf webcam, eliminating the need for costly infrared eye-tracking hardware or cloud-based processing. By performing gaze analytics directly on the display, RAEMAP-Display preserves user privacy while delivering real-time insights into audience attention across environments such as retail stores, healthcare facilities, transportation hubs, and fuel stations. The platform continuously analyzes viewer engagement and adapts advertising or informational content to maximize effectiveness, creating a closed-loop system that improves content performance without manual intervention. This capability enables new engagement-based business models in which advertisers can measure return on investment using verified audience attention while display operators generate revenue based on actual engagement rather than static advertising contracts. The project will advance the technology through prototype refinement, real-world pilot deployments, and commercialization activities designed to validate performance, demonstrate market value, and support industry adoption. By transforming affordable computer vision research into a scalable commercial platform, RAEMAP-Display has the potential to redefine digital signage by providing organizations with privacy-preserving audience analytics and creating new revenue opportunities through intelligent, data-driven content delivery.

- *Automated Building Safety, Code Compliance, and Cyber-Physical Asset Tracking*; Dr. Arsalan Heydarian, UVA. InspectAI is an artificial intelligence platform designed to modernize commercial building inspections by automating code compliance assessments and improving the consistency, speed, and accuracy of inspection workflows. Developed through years of federally funded research, the platform combines computer vision, vision-language models, and building knowledge graphs to analyze smartphone images collected during facility walkthroughs and generate evidence-based inspection reports linked directly to applicable building codes. In addition to identifying structural and code compliance issues, InspectAI can detect and track network-connected building control systems over time, helping facility owners better manage cybersecurity risks associated with aging infrastructure. The technology addresses growing workforce shortages among building inspectors while reducing the time and expertise required to perform complex commercial inspections. The project is advancing the platform through pilot deployments with university facilities, expansion of its commercial building code knowledge base, and development of production-ready mobile and web applications. Customer discovery activities with facilities managers, commercial inspectors, industry partners, and Department of Defense stakeholders will guide product development and commercialization strategy while supporting future SBIR and venture funding opportunities. By transforming AI research into a practical inspection platform, InspectAI has the potential to improve infrastructure management, strengthen building safety and cybersecurity, and accelerate the adoption of intelligent inspection technologies across commercial, institutional, and government facilities.
- *CAPTCHA: Completely Automated Physical test to tell Computers and Humans Apart*; Dr. Mingkui Wei, Mason. CAPTCHA (Completely Automated Physical Test to Tell Computers and Humans Apart) is a next-generation human verification technology designed to address the growing inability of traditional CAPTCHA systems to distinguish humans from increasingly capable AI-powered bots. Rather than relying on puzzles that have become both frustrating for users and vulnerable to automated solving, CAPTCHA leverages the fundamental difference between humans and software: humans interact with the physical world, while bots operate entirely within the digital environment. The technology securely delivers verification challenges that can only be perceived on a physical display, preventing automated programs from accessing the challenge regardless of their computational capabilities. This approach enables a significantly simpler and more user-friendly verification experience while providing stronger protection against automated attacks such as credential abuse, fraudulent account creation, data scraping, and spam. The project will advance the technology through prototype development, validation, and commercialization activities supported by a growing intellectual property portfolio, including multiple provisional patents and an international patent application. With the global demand for bot mitigation continuing to grow, CAPTCHA has the potential to redefine online human verification by providing organizations with a more secure, scalable, and user-friendly alternative to conventional CAPTCHA technologies while strengthening the security of websites, online services, and

digital platforms.

- *AgentSec: Agentic AI Security Gateway*; Dr. Rui Ning, ODU. AgentSec is a cybersecurity platform designed to secure the growing ecosystem of agentic artificial intelligence systems that autonomously interact with enterprise applications, databases, and software tools. As organizations increasingly deploy AI agents to automate complex workflows, these systems become vulnerable to prompt injection attacks and other threats that can manipulate AI behavior or misuse connected resources. AgentSec addresses this challenge by serving as a centralized security gateway that applies consistent, enterprise-defined policies to every AI agent, governing how agents access data, invoke tools, and perform high-impact actions. The platform combines pre-deployment security validation with real-time monitoring and policy enforcement to detect unsafe configurations, prevent unauthorized tool use, and generate audit-ready records that support AI governance and regulatory compliance. Rather than requiring organizations to build custom safeguards for each AI application, AgentSec provides a scalable security framework that can be deployed across multiple agents, workflows, and enterprise environments. The project will advance the technology through customer discovery, pilot deployments, industry partnerships, and commercialization activities while exploring intellectual property protection and follow-on funding opportunities. By providing organizations with a practical approach to securing AI-powered automation, AgentSec has the potential to accelerate the safe adoption of agentic AI, reduce cybersecurity risk, and establish a commercial platform for enterprise AI governance and security.
- *HGNSense: Personalized Impairment Detection through Secure AI-Driven Horizontal Gaze Nystagmus Analysis* Dr. Ahmad Salman, JMU. HGNSense is an AI-powered impairment detection platform that uses Horizontal Gaze Nystagmus (HGN), a well-established physiological indicator of fatigue, intoxication, and neurological impairment, to provide objective assessments of operator readiness. Using high-resolution cameras and machine learning algorithms running on secure edge devices, the platform establishes individualized physiological baselines and evaluates impairment relative to each user's normal condition rather than relying on generalized thresholds. This personalized approach improves accuracy while reducing false positives and preserving user privacy by processing biometric data locally instead of transmitting it to centralized databases. Designed for applications including advanced driver assistance systems, commercial fleets, law enforcement, industrial safety, and sports medicine, HGNSense addresses the growing demand for reliable, non-invasive impairment detection technologies that support safety and regulatory compliance. The project will advance the technology toward commercialization through prototype development, cybersecurity and regulatory validation, customer discovery, and pilot deployments with prospective industry partners. Future commercialization efforts include integration with vehicle manufacturers, fleet management platforms, and occupational health providers through licensing and software-plus-hardware business models. By combining artificial intelligence, edge computing, and privacy-preserving biometric analysis, HGNSense has the potential to improve public safety, reduce organizational liability, and accelerate the adoption of objective impairment detection technologies across transportation, healthcare, and other safety-critical industries.
- *From RFIDs to mmIDs: 5G-native Batteryless Tags for Tracking and Communication*. Dr. Parth Pathak, Mason. mmID is a batteryless Internet of Things (IoT) technology that enables precise location tracking, sensing, and communication for next-generation smart factories, warehouses, and automated supply chains. As industrial facilities increasingly rely on autonomous robots and connected devices, the need for low-maintenance, energy-efficient sensing technologies continues to grow. Unlike conventional IoT devices that require periodic battery replacement, mmID uses ultra-low-power backscatter communications and energy-efficient millimeter-wave technology to operate for extended periods while delivering significantly greater localization accuracy than traditional RFID or Bluetooth systems. Compatible with emerging 5G, future 6G, and next-generation Wi-Fi networks, the platform can be integrated into existing wireless infrastructure without requiring costly new deployments. The technology enables real-time, high-precision tracking of inventory, equipment, and robotic systems, supporting more efficient warehouse operations, manufacturing, and logistics. The project will advance mmID through prototype refinement, industry validation, and commercialization activities, with a focus on demonstrating its performance in real-world industrial environments and preparing the technology for market adoption. By eliminating the need for battery replacement while improving

the accuracy and scalability of industrial sensing, mmID has the potential to reduce operating costs, improve sustainability, and accelerate the deployment of intelligent automation across manufacturing, warehousing, and supply chain industries.

ASCEND Fund Supported Innovations

- *Advancing LLM and Agentic AI for Telecom Networks* Dr. Cong Shen, UVA and WiSights Lab. WiSights Lab is developing an AI-powered network operations platform that helps telecommunications providers manage increasingly complex 5G, Open RAN, and next-generation 6G infrastructure. As modern telecom networks become more software-defined and distributed, operators face growing cybersecurity risks, rising operational costs, and a shortage of engineers capable of managing multi-vendor environments. The platform builds on proprietary research in telecom-specialized large language models (LLMs) and agentic AI to create intelligent assistants that understand industry standards, analyze real-time network telemetry, and support critical operational tasks such as root-cause analysis, configuration validation, anomaly detection, and cybersecurity incident response. Unlike general-purpose AI tools, the platform is purpose-built for telecommunications environments, enabling more reliable, context-aware decision support while maintaining human oversight of network operations. The project will advance the technology by developing a pilot-ready platform, conducting customer demonstrations, and validating with telecommunications operators and industry partners to accelerate commercialization. Future efforts will focus on pilot deployments, enterprise software licensing, expansion across cloud-native and Open RAN ecosystems, and protection of the company's intellectual property portfolio. By transforming advanced AI research into a practical operational platform, WiSights Lab aims to reduce network downtime, improve service reliability, strengthen cybersecurity, and enable more efficient management of next-generation communications infrastructure while positioning the company to compete in the rapidly growing market for AI-driven telecom operations.
- *Data-Centric Security for Adversarial-Resilient Radio Frequency Machine Learning* Dr. William Headley, VT National Security Institute and Hardshell AI. This project advances a new cybersecurity capability designed to protect radio frequency (RF) artificial intelligence and machine learning systems from attacks that compromise the data used to train and operate them. As RF AI technologies become central to applications such as counter-uncrewed aircraft systems, spectrum monitoring, electronic warfare, and next-generation wireless communications, they face growing risks of adversarial manipulation of training data and RF signals, which can degrade system performance or undermine trust in AI-driven decision-making. Building on applied research at the VT National Security Institute and in partnership with Hardshell AI, the project will develop techniques to detect and mitigate data-centric attacks targeting RF machine learning systems, addressing a critical security gap not covered by existing commercial spectrum monitoring products. The technology will be evaluated across practical RF applications, including spectrum sensing, signal classification, and emitter identification, with the goal of establishing measurable performance benchmarks and creating a commercially deployable security framework. The project will also support the integration of the technology into Hardshell AI's commercial product portfolio, strengthen the underlying intellectual property, and validate market demand. By improving the trustworthiness and resilience of AI-enabled RF systems, the technology has the potential to support defense, telecommunications, and critical infrastructure markets where secure spectrum operations are increasingly essential, positioning the partnership for follow-on federal funding and commercial deployment in a rapidly expanding market for AI-enabled wireless security.
- *AETD-X: AI-Based Early Warning System for Inappropriate EMR Access* Dr. Michael Lapke, CNU, and Neptune Shield. AETD-X is an AI-powered cybersecurity platform that helps healthcare organizations detect inappropriate or anomalous access to sensitive electronic medical records (EMRs) in real time. While healthcare providers have strengthened network security, existing access monitoring tools largely rely on static rules and retrospective audits that often fail to identify subtle misuse of legitimate credentials or contextually inappropriate data access. AETD-X addresses this challenge by applying advanced artificial intelligence to learn normal clinical workflows and continuously evaluate user behavior within its operational context. Using transformer-based sequence modeling, context-aware anomaly detection, probabilistic risk scoring, and explainable AI, the platform identifies unusual

access patterns and provides transparent, actionable insights that support compliance and incident response. The technology is designed to integrate with leading EMR platforms via secure application programming interfaces (APIs), enabling healthcare organizations to strengthen data protection and reduce the administrative burden of manual audits and compliance reviews. The project will advance the platform from research validation to a production-ready solution through customer discovery, pilot partner engagement, prototype refinement, and preparation for follow-on commercialization funding. Developed in partnership with Neptune Shield, the technology has the potential to transform healthcare data security by shifting organizations from reactive compliance auditing to proactive, AI-driven data access assurance, improving patient privacy, reducing cybersecurity risk, and supporting the secure management of sensitive clinical information.

- *BEHOLDER: Non-Invasive Timing-First Cyber Event Detection for Substation Gateways and Edge Compute* Dr. Matt Jablonski, Mason and SARC Solutions. Beholder [for Utilities] is a non-invasive cybersecurity monitoring platform designed to improve visibility into substation gateways and edge-computing devices that support modern electric grid operations. As utilities expand the use of distributed monitoring and remote-control technologies, many operational technology (OT) devices remain difficult to secure with traditional endpoint detection tools due to constrained hardware, proprietary software, and limited system logging. Building upon prior collaborative research between Mason and SARC Solutions, the platform analyzes device behavior through execution timing and other passive sensing techniques to detect cyber events without disrupting critical utility operations. The project will focus on commercializing this technology for electric utility environments by validating customer needs, refining deployment architectures, and developing repeatable demonstrations that showcase the platform's value for substation cybersecurity. Working with industry partners, the team will define practical integration pathways for security operations centers, produce reference architectures tailored to utility environments, and create commercialization assets that support engagement with prospective customers. The project also establishes a pathway toward technology maturation through the Department of Energy's Innovation Crossroads program and future pilot deployments with utility partners. By translating advanced cyber-physical security research into a utility-ready product, Beholder for Utilities has the potential to strengthen grid resilience, improve incident detection and response, and provide electric utilities with practical tools for protecting increasingly connected operational technology infrastructure.
- *PointerPass: First-Pass DFIR Evidence Pointing for Modern Forensic Labs* Dr. Victor Oleson, VCU and DeepRunAI Labs. PointerPass is an AI-assisted digital forensics platform that accelerates the initial review of digital evidence by helping investigators quickly identify relevant leads while preserving established forensic workflows. As law enforcement agencies and digital forensics laboratories face increasing volumes of evidence and persistent staffing shortages, case backlogs continue to delay investigations and increase operational risk. PointerPass addresses this challenge by performing secure, offline first-pass analysis of acquired digital evidence within controlled laboratory environments, producing evidence-backed pointers that help examiners prioritize their investigations without replacing expert judgment or making evidentiary conclusions. The platform combines semantic search, structured data extraction, and AI-assisted analysis to rapidly identify relevant records, media, and other digital artifacts while maintaining traceability and provenance throughout the review process. Building on a successful proof-of-concept validated with law enforcement partners, the project will advance the technology by developing a deployment-ready pilot package, standardized reporting capabilities, and customer validation with prospective public safety partners. Commercialization activities will focus on demonstrating measurable reductions in investigation time, validating operational value through pilot deployments, and refining product packaging and pricing for digital forensic laboratories. By transforming AI research into a practical investigative support tool, PointerPass has the potential to reduce digital evidence backlogs, improve investigators' efficiency, and strengthen public safety organizations' ability to manage rapidly growing volumes of digital evidence while maintaining rigorous forensic standards.
- *Responsible AI Governance through Cognitive Hardware Monitoring* Dr. Khaled Khasawneh, Mason and SecureMind Technologies, Inc. Hardware-Enabled Mechanisms (HEMs) is a hardware-based AI

governance platform that provides trusted oversight of artificial intelligence training and inference workloads. As AI adoption accelerates across defense, healthcare, critical infrastructure, and commercial industries, organizations face increasing pressure to ensure AI systems comply with security policies, resource constraints, and emerging regulatory requirements. Existing governance approaches rely primarily on software controls that can be bypassed or lack visibility into the underlying hardware executing AI workloads. HEMs addresses this gap by combining trusted hardware security technologies with monitoring and attestation capabilities that verify AI operations at the chip level, enabling organizations to enforce governance policies with greater assurance. Building on proven research in hardware security and microarchitectural monitoring, the platform extends these capabilities to AI systems by integrating hardware-level protections with emerging AI governance frameworks. The project will advance the technology through prototype development, performance validation, and extensive customer discovery with AI developers, cloud service providers, semiconductor companies, and government stakeholders to refine product requirements and commercialization strategy. Future efforts will focus on strategic partnerships, licensing opportunities, and follow-on funding to support product development and market deployment. By establishing a trusted hardware foundation for AI governance, HEMs have the potential to improve the security, transparency, and regulatory compliance of AI systems while enabling organizations to deploy advanced AI technologies with greater confidence across mission-critical environments.

4.2.2 SWVA Node

CCI SWVA seeks to promote innovation and commercialization of technologies supported at early stages by CCI SWVA seed investment. The node oversees two formal programs in support of this goal: the Innovation: Ideation to Commercialization (IIC) Program, which seeks to help researchers translate their academic research into viable, market-ready products; and the Cyber Innovation Scholars (CIS) Program, which seeks to provide an introduction to concepts of commercialization for graduate students enrolled in CCI member institutions.

Ideation to Commercialization Program

Ideation to Commercialization (IIC) projects should focus on translating lab work into 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.

Selection Criteria

Concept Maturity (30%)

- 1. Prior work with or letter of commitment from startup
- 2. Demonstration of documented progress toward commercialization, including data or prototype availability

Commercialization and Market Potential (20%)

- 1. How the proposed technology will meet clearly defined problem/unmet need
- 2. Technical feasibility
- 3. Market size or opportunity
- 4. Strength of competition and competitive products

- 5. Ability of proposed solution to capture market share and secure long-term competitive advantage including IP protection

Development Plan and Budget (10%)

- 1. Clear and appropriate budget that aligns with technology development plan or startup engagement
- 2. Milestones have specified dates and concrete deliverables
- 3. Scientific/development methods are valid

Value of the Funding (20%)

- 1. Commercialization funds will move technology to clearly defined inflection point
- 2. Achievement of milestones will de-risk technology and/or validate market opportunity
- 3. Funds will have proportional impact on moving technology forward with CCI goals

Alignment and Qualifications (20%)

- 1. Relevance to CCI focus areas
- 2. Strength, relevant experience, and engagement of team

Innovation Grants Awarded

CCI SWVA awarded 6 awards for projects originally proposed in FY25. Joining these 6 were 3 new awards issued in response to the FY26 call for proposals highlighted above. Lastly, 2 award supplements were issued to in-progress awards that required support beyond the original proposal to achieve noteworthy commercialization milestones. All awards were issued to VT for periods of performance falling in FY26.

Ideation to Commercialization Awarded Projects

- *Securing Eye-Tracking Data from Side-Channel Attacks in Virtual Reality Systems*, Dr. Brendan David-John and Dr. Bo Ji, VT. The technology developed in this project supports securing emerging virtual, augmented, and mixed-reality (XR) devices. Prior research from our team has revealed that third-party applications can reconstruct sensitive sensor data collected by the headset when they don't have direct access to that sensor. This kind of attack uses a benign system signal, such as frames per second, to leak sensitive sensor data which is called a side channel. Specifically, we found that XR systems using eye-tracking data for rendering optimizations expose a side channel that leaks gaze data. Our project explored additional attacks that are more sophisticated in leaking gaze data through low-level system performance counters in ways that cannot be detected, and leads to a new technology capable of detecting and eliminating these side channels through 3D graphics software and drivers. Our technology is still in the design and development phase prior to a robust validation against realistic XR workloads and attacks.
- *DID Calendar Launch*, Dr. Christiana Garcia, VT. This project is developing an open-source, decentralized calendar platform designed to improve how scientific communities coordinate activities, establish trust, and share opportunities. The technology supports Decentralized Science (DeSci), an emerging approach that uses open digital infrastructure to make research collaboration, attribution, and access more transparent and community driven. Today, researchers often rely on disconnected calendars, websites, mailing lists, and commercial platforms to find seminars, deadlines, workshops, data-collection opportunities, and collaborative events. These systems can create duplicated information, limited interoperability, uncertain ownership of records, and dependence on a single service provider. The proposed platform addresses these barriers by combining a familiar calendar interface with decentralized identifiers (DIDs) and blockchain-enabled verification mechanisms. A DID is a cryptographically verifiable digital identifier that can represent a person, research group, institution, project, dataset, or event without requiring reliance on a centralized identity provider. DIDs can be

resolved to digital documents containing public verification material and approved service endpoints, enabling more trustworthy digital interactions. Within the calendar platform, this approach can help users verify the source and provenance of event information, associate events with persistent research identities, and retain greater control over their own records and affiliations. The platform is being developed as open-source software to encourage broad adoption, technical transparency, interoperability, and community contribution. Potential users include university researchers, student organizations, research centers, scientific societies, funding and innovation communities, and interdisciplinary collaborators. By bringing verifiable identity and decentralized records into everyday research coordination, the technology aims to reduce friction in scientific collaboration and help create a more open, resilient, and trusted research ecosystem.

- *SmartHomeSecure: A GenAI-Powered Prototype for Detecting Defects and Vulnerabilities in Smart Home Automation Systems*, Dr. Xinghua Gao, Myers-Lawson School of Construction, and Dr. Na Meng, Department of Computer Science, VT. SmartHomeSecure is a generative-AI-enabled software technology designed to make smart home automation safer, more reliable, and easier to manage. Modern platforms such as Home Assistant rely heavily on YAML configuration files—human-readable instructions that define how connected devices should behave. Small mistakes in these files can cause automations to fail, behave unpredictably, or create security and safety risks. The CCI-supported project originally envisioned an integrated tool for detecting configuration defects and security vulnerabilities and for testing automations through simulation. The resulting SmartHomeSecure prototype demonstrates a core part of that vision: automated detection and repair of configuration errors. The system combines lightweight program analysis with constrained large language model (LLM) generation. It first parses a user’s configuration, identifies the location and type of an error, and applies deterministic fixes when possible. For more complex cases, it provides the LLM with structured error information and strict repair constraints so that the model produces a minimal, valid correction rather than freely rewriting the configuration. Evaluation on 100 real-world Home Assistant YAML files containing five common categories of injected errors showed strong performance. Three tested models achieved 100% error-detection accuracy, while successful repair rates ranged from 87% to 93%. Manual review found no hallucinated or incorrect changes among successful repairs. These results show how combining software analysis with generative AI can deliver practical, trustworthy assistance for smart-home users and provide a foundation for broader cybersecurity and automated testing capabilities.
- *Virtual Reality–Augmented Digital twin for grid security Operator Training (VR-ADOPT)*, Dr. Ali Mehrizi-Sani, Bradley Department of Electrical and Computer Engineering, VT. Power system workforce training is becoming increasingly urgent as experienced personnel retire faster than new engineers, technicians, and operators are trained. At the same time, the grid is rapidly evolving, requiring the workforce to understand new technologies such as inverter-based resources, distributed generation, automation, communication systems, and other technologies that were not widely deployed in their current form even a decade ago. Existing training methods remain largely lecture-based, with hands-on components that are typically limited to small, simulated test systems and artificial user interaction. To address this gap, we are developing a virtual reality (VR)-based operator training platform built around a digital twin of power system infrastructure, including control rooms, substations, and transmission assets. The platform combines immersive VR visualization with physics-based power system simulation, allowing trainees to interact with equipment and controls and observe the system-level consequences of their decisions in real time. Actions such as operating breakers, responding to alarms, or executing switching procedures are reflected in the underlying simulation, which in turn updates voltages, power flows, equipment states, and operating conditions within the virtual environment. The system can also incorporate visually identical operator interfaces and generate training scenarios involving outages, protection events, communication failures, or abnormal grid conditions. Similar to a flight simulator, the platform provides a safe, repeatable, and authentic environment for developing situational awareness and operational judgment.
- *Defining a New Standard for IIoT Wireless Security*, Dr. Alan Michaels, National Security Institute, VT. HOPS (High Order PSK Signaling) is a proprietary spread-spectrum waveform designed for secure, resilient, low-latency wireless communications in congested and contested RF environments. Unlike

conventional direct-sequence spread spectrum, HOPS uses arbitrary phase relationships within the spreading waveform, creating a highly flexible signaling structure that supports robust multiple-access operation, while making efficient shared use of spectrum and transmit energy. Its MAC architecture employs receiver-assigned CDMA, allowing multiple users to transmit simultaneously, without scheduling. This enables dense networks with minimal coordination overhead and supports a design philosophy in which nodes remain off the air whenever possible. HOPS is intended to scale across a wide range of data-rate and networking requirements. Current implementations support 50 kbps, with planned upgrades to roughly 250 kbps, while maintaining sub-millisecond latency for suitable traffic classes. The waveform is well suited to point-to-point, point-to-multipoint, hierarchical, relay, and mesh networking architectures. Beyond data communications, HOPS can support precision timing transfer, providing a potential GPS-independent mechanism for synchronizing distributed systems. Its combination of low latency, scalable multi-user access, resilience, security, and timing capability makes it attractive for industrial IoT, critical infrastructure, defense, logistics, and other applications where conventional wireless links may be inadequate.

- *OpenAgents: A Secure Low-Code Platform for Scalable Multi-Agent AI Deployment*, Dr. Xuan Wang, VT. Artificial intelligence (AI) agents can help organizations automate complex tasks, from processing documents to analyzing data and coordinating specialized software tools. However, many existing AI systems rely on external cloud services, creating challenges for organizations that handle sensitive information or operate in environments with limited internet connectivity. Supported by the Commonwealth Cyber Initiative, our project is developing OpenAgents, a secure, low-code platform that enables organizations to build and deploy AI agents on their own computing infrastructure. Instead of relying on large cloud-based models, OpenAgents uses smaller language models and coordinates specialized agents to complete complex tasks. This approach is designed to keep sensitive data under an organization's control while reducing the computing resources needed for AI-powered automation. Security is built into the platform's design. OpenAgents will execute AI-generated actions in isolated environments, check code for potentially dangerous behavior, enforce resource limits, and provide monitoring and audit capabilities. A planned visual interface will also allow users with limited programming experience to create and manage AI workflows. Potential applications include automating clinical workflows, processing financial documents, and supporting secure data analysis for government and defense organizations. Through framework development and pilot deployments with Virginia organizations, the project aims to evaluate the technology's security, performance, and practical usability. Ultimately, OpenAgents seeks to make advanced AI automation more accessible to organizations that need greater control over their data and computing environments.
- *Accelerating Micro-Mechanical Innovation: High-Throughput GHz Vibrometry for Next-Gen Communication, Defense, and Quantum Engineering*, Dr. Yizheng Zhu, VT. The proposal describes a new scientific instrument for measuring tiny vibrations in miniature electronic and mechanical devices. These vibrations are important in technologies such as 5G communication equipment, radar, autonomous vehicles, medical devices, and quantum sensors. Today, engineers often use laser-based tools that measure only a small range of frequencies, require complicated setup and calibration, and can take many hours or days to examine a single device. The proposed technology uses special optical design to detect vibrations without touching or damaging the device. It can examine a much wider range of vibration frequencies, potentially up to approximately 110 gigahertz, and collect detailed information within just a few minutes, much faster than existing commercial systems. It also does not rely on powerful lasers or require specialized ultra-fast detectors, and is less affected by changes in operating environment. In practical terms, the system acts like a high-speed, highly sensitive stethoscope for miniature devices. It can show where a device is vibrating, how strongly it is moving, and how its vibrations change across different frequencies. This could help engineers design, test, and improve advanced components more quickly while reducing manufacturing costs. The team is now working toward a commercial prototype, customer testing, company formation, and early funding.

Cyber Innovation Scholars Program

Led by assistant director Mr. Mark Mondry, this program introduces graduate student applicants to the possibilities for commercializing cybersecurity research. CCI SWVA selected 50 doctoral candidates, master's students, and postdoctoral researchers for invitation to the Cyber Startup Boot Camp, where they were introduced to processes involved in commercializing cyber technology. The 2026 Cyber Innovation Scholars hail from departments across VT, including business information technology, computer science, electrical and computer engineering, environmental design and planning, marketing, mathematics, and physics. 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 VT's LAUNCH and associate director for partnerships and engagement at CCI SWVA, the workshop combined seven hour-long startup labs into a half-day marathon, covering some of the most critical issues to consider before creating a startup. Of the 50 enrollees, 47 attended and completed the workshop and were awarded \$1,500 of funding each for professional development and exploring commercialization potential for their research.

4.2.3 CVN Node

Dreams 2 Reality Incubator (D2RI)

CVN awarded three commercialization projects in FY26 through its Dreams to Reality Incubator (D2RI), at \$30,000 each, totaling \$90,000. The projects were awarded internally, with performance beginning 1 January 2026, and are funded from FY26 appropriations. D2RI funds the stage between technically promising research and market application: identifying potential customers, understanding the value they would place on a solution, and defining the validation required for adoption. Conventional research awards are designed to produce scientific results rather than commercial evidence, so this stage often goes unfunded. All three FY26 projects are led by VCU faculty and span advanced manufacturing security, operational technology workforce training, and digital health.

Awarded Projects

- Machine Tool Anomaly Detection (MADe), Dr. Jayasimha Atluasimha, VCU.
- SleuthCPS: A Capture-the-Flag and Incident Response Training Platform for Industrial Control and Operational Technology Environments, Dr. Irfan Ahmed, VCU.
- Diabetic Smart Socks, Dr. Christina Tang, VCU.

Invention Disclosure

Diabetic foot ulcers cost the U.S. health care system an estimated \$9-13 billion annually, and a sustained temperature difference between a patient's feet is a recognized early warning sign. Dr. Tang's team is developing socks that change color with skin temperature, paired with a smartphone application that reads the color difference between the left and right foot to flag elevated ulcer risk.

During the reporting period, the team formulated thermochromic liquid crystal coatings and selected a horizontal-line application method for better adhesion and color consistency. It developed an image-processing algorithm that infers temperature difference from color change, achieving an R^2 of 0.842 against thermocouple measurement with a mean absolute error of 0.089°C, along with automated detection of the relevant regions on a three-dimensional model foot. The team filed an invention disclosure on this quantitative imaging approach.

The team also began early market validation. Prototypes were displayed through the Shelfie Program at the VCU Shift Retail Lab, where 20 consumers provided structured feedback: 60 percent indicated willingness to pay \$20–\$50 per pair, 65 percent preferred coin-sized or larger indicator patches, and 75 percent indicated willingness to complete a measurement routine of three minutes or longer. The project supported three VCU students, one master's researcher, and two undergraduates.

Chapter 5

Collaborative Partnerships and Projects

5.1 Hub Partnerships

5.1.1 Industry-led Consortia

Industry/University Cooperative Research Centers

CCI faculty currently lead two Industry-University Cooperative Research Centers (IUCRCs), co-funded by 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, and the Cyber SMART IUCRC focuses on cybersecurity solutions. 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 VT, Mason, and the University of Arizona. Dr. Gretchen Matthews, CCI SWVA Node Director, also serves as site director at VT 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. Approximately 30% of the research funding that CCI researchers attract comes from the private sector and partnerships, such as the ones described here.

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 Node Partnerships

5.2.1 CVN Node

Academic

- Dr. Vullikanti's team collaborated with data.org through the Privacy-Enhancing Technologies Challenge for public health.
- Dr. Ul Hassan's AR/VR provenance project collaborated with the University of Maryland, Baltimore County, which sent a visiting summer undergraduate researcher who contributed without award funding and is the first author on the resulting manuscript. Dr. Qian's radar security work was conducted in collaboration with Professor Ish Kumar Jain at Rensselaer Polytechnic Institute, whose team supported real-world experimentation on their IBM PAAM software-defined radio testbed. Dr. Zhang's autonomous driving project produced its offline-to-online reinforcement learning result with collaborators at Duke University. Dr. Dinh's project worked with the Faculty of Information Technology at VNU University of Engineering and Technology in Hanoi and with Dr. Bon Trinh of the UVA Department of Pathology on hardware-efficient encodings for quantum annealers; those partners were supported by Vietnam NAFOSTED, extending the reach of the CCI investment at no additional cost to the commonwealth.

Industry

- CVN internships continue to generate industry partnerships, concentrated among small and locally owned businesses in the greater Richmond area. FY26 host organizations included Deep Run AI Labs, AMC Technology, Hive Systems, Spanalytics, IT4Causes, Weinstein Properties, Virginia Farm Bureau, GRTC, and the State Corporation Commission. Through UVA, additional partnerships included Booz Allen Hamilton, Archibald Corporation, Skillbit Labs, Hardshell, Venture Central, and IMCI Technologies, with AWS, Amazon, MITRE, Accenture, and CapTech participating in the AI Academy employer exhibition.
- Dr. Dinh's quantum cloud project maintains a research collaboration with D-Wave Quantum, whose Advantage and Advantage2 topology data were used to validate every attack and defense result, ensuring the findings speak to deployed commercial hardware rather than an idealized model. Through the node's commercialization and research awards, FY26 also engaged partners in the semiconductor and memory technology sector: Everspin, Western Digital, Hprobe/Mycronic, and Numem, alongside domain experts at IBM, NIST, and CEA-Spintec, through Dr. Atulasimha's NoMagField customer-discovery work.
- Dr. Ul Hassan's AR/VR provenance project submitted two Department of Energy proposals under the Genesis Mission call, each seeking \$750,000 for scientific AI integrity monitoring; both were declined. Dr. Alemzadeh's concluding EMS project reported two further unsuccessful bids, a \$1,800,000 National Institutes of Health proposal and a \$233,000 NSF proposal, both with resubmissions pending. Dr. Dinh's quantum cloud project reported four unsuccessful proposals totaling \$1,659,404 requested to NSF, the U.S. Department of Energy, and two Sony programs, all of which the PI reports remain active for resubmission. Recording them here reflects the node's investment in pursuing substantially larger federal awards, regardless of whether each bid succeeds.

Government

- Richmond Department of Public Utilities — engaged through a separate CVN-scoped project (award index 580070) on which Dr. Dinh is PI and Dr. Atulasimha is co-PI, addressing water infrastructure

security; this is distinct from Dr. Dinh’s highlighted FY26 quantum-cloud award, which does not reference this partnership.

- FCC, Office of Engineering and Technology — Cypher-Bridge fellowships, supporting FCC spectrum policy and enforcement work through applied AI tooling.
- Virginia State Police — Cyber4n6.
- NASA — partner on the open-source UAV simulation testbed developed under Dr. Alemzadeh’s concluding EMS project; public release of the testbed is pending partner confirmation.

5.2.2 CoVA Node

Industry

CoVA CCI collaborates with academic institutions across the state on cybersecurity research projects previously mentioned in this report. Researchers are also partnering with businesses on potential federal funding opportunities and ongoing research. Some of these partners include:

- G2Ops
- MITRE
- MI Technical Solutions
- Port of Virginia
- Valor Cybersecurity
- Peregrine Technical Solutions

All projects funded through CoVA CCI involve collaborations with researchers from multiple institutions and/or business partners.

Government

During FY26, CoVA CCI, in partnership with ODU, the City of Virginia Economic Development Office, and the Information Technology Office, held discussions about creating strategic partnerships to promote the City of Virginia and Hampton Roads to business partners. They also aimed to work with students on developing internships and potential jobs. After several meetings with key stakeholders, three working groups were established: Strategic Partnerships, Workforce Development, and IT Infrastructure. This initiative has led to a series of meetings with both national and international companies interested in investing in and expanding their presence in the region.

5.2.3 NoVA Node

Collaborative Programs

Cybersecurity Traineeship Program Partners

Mason, NVCC, Peraton, Auspex Labs, Rapid Prototyping Research Center, Inspired Solutions, Solvitur Systems.

Undergraduate Internship Program Partners

Mason, JMU, UMW, NVCC, Blue Ridge Community College, Blue Sky Innovators, Critical Shift Corporation, EngineerRD, Great Victory Legends, Summit Knowledge Solutions, SyncData AI, RPRC, TekScope.

High School Cybersecurity Internship Program Partners

Mason, Northern Virginia Science Center Foundation, Appian, CGI Federal, Chainbridge Solutions, Deltek, F1 Cloud Solutions, GT Edge AI, Leidos, Maximus, NT Concepts, Obscurity Labs, Oceus Networks, Pingwind, SES, SixGen, Solvitur Systems, Tyrula LLC, Unissant, VT Thinkabit Lab.

5.2.4 SWVA Node

Collaborative Partnerships

CCI encourages collaboration with industry, state partners, and stakeholders for all our funded programs. We highlight here a few of the standout achievements of note in FY26:

- CCI SWVA Director Dr. Gretchen Matthews continues to engage with industry members of the NSF Industry-University Cooperative Research Centers (IUCRC) Cyber SMART, which include Comcast, Digital Garage, Washington Core, Financial Services Agency of Japan, IQI Balanced Intelligence, Irys, NEC America, Sumitomo Mitsui Trust Bank, and Triple Point Security through her role as Cyber SMART Site Director. Cyber SMART's academic sites are Georgetown, Notre Dame, VT, and the University of Technology Sydney. VT hosted its Spring 2026 Industrial Advisory Board meeting on April 10 in Alexandria, VA.
- VT's Dr. Ali Mehrizi-Sani established a new Blacksburg-based training startup called Amber & Arc LLC in August 2025. This firm utilizes VR technology supported by CCI and, in collaboration with VT Intellectual Property (Link, License, Launch), specializes in power systems consulting, training, and education.
- CCI SWVA Associate Director for Research Dr. Alan Michaels's private venture, Tokay Systems LLC, secured external federal funding through the NSWC Dahlgren // Joint Intermediate Force Capabilities Office through a \$350,000 award to VT with Tokay Systems as a subcontractor.

In addition, several other funded programs engage with government and corporate partners to continue promoting cybersecurity and cyber-adjacent initiatives.

- VMI's Dr. Abdelhamid continues to work with the Lexington-based cybersecurity startup Network Sense, which he founded.
- Radford University's Tom Bennett, recipient of the 2025 CCI Impact Award, partnered with the City of Winchester to have their personnel strengthen their cybersecurity knowledge and skills.
- Dr. Tom Hou, in part due to his IIC award in FY26, is growing connections with Rockville, MD-based firm "Nexcepta" which provides innovative technical solutions, mission-critical capabilities, and commercial products, along with tailored R&D and engineering services for federal and commercial clients, and features several former VT faculty.
- CCI SWVA Director Dr. Gretchen Matthews is partnering with Fujitsu Research of America after its demonstrated interest in her work in quantum error correction.
- Dr. Mehrizi-Sani is also the Lead Power Systems expert for Quadrante Right Analytics, an international firm with 38 offices worldwide.
- Dr. Linbo Shao from VT is in connection with the Toyota Research Institute in Ann Arbor, Michigan, in preliminary discussion regarding applications of his research for the automotive manufacturer.
- Dr. Yaling Yang expanded ties with the GSM Association, an advocacy and lobbying organization for the mobile communications industry.
- Yizheng Zhu is working with Blacksburg-based startup Tern Photonics, focusing on development and manufacture of state-of-the-art optical vibrometry products and services to industry and research institutions in wireless communication, MEMS, quantum engineering, and more.

5.3 Correlated Economic Outcomes

Every two years, CCI commissions RTI International to conduct an Economic Impact Study to highlight CCI's role in Virginia's cybersecurity economy and the economic contributions of its research, workforce development, and commercialization activities. The next study will be conducted in FY27 and cover fiscal years 2026 and 2027. Economic impact findings and data for FY26 will be included in the CCI FY27 Annual Report.

5.3.1 CCI Hub

In FY26, the CCI Hub employed 33 Graduate Research Assistants and Interns to conduct cybersecurity research under the direction of the Hub research faculty and operate and maintain the CCI xG Testbed under the direction of the xG Testbed Director.

CCI also supported and funded 16 students to work on projects for CACI, GuidePoint Security, Public Broadcasting Systems, and LMI as part of the Project-Based learning program.

5.3.2 CVN Node

Research Training

- At least 26 graduate research assistants conducted research under the direction of a faculty advisor on CVN-supported projects, along with at least 11 undergraduate researchers and 1 postdoctoral associate. Figures are drawn from technical reports submitted during the reporting period and include both active FY26 awards and prior-cycle awards that concluded during the period.

Internships

- At least 26 graduate research assistants conducted research under the direction of a faculty advisor on CVN-supported projects, along with at least 11 undergraduate researchers and 1 postdoctoral associate. Figures are drawn from technical reports submitted during the reporting period and include both active FY26 awards and prior-cycle awards that concluded during the period.

Student Training Programs

- 35 students trained through the UVA AWS AI Academy, a five-day immersive program in AI and machine learning for cybersecurity delivered with Amazon Web Services and Booz Allen Hamilton.
- 36 participants completed the Digital Forensics Challenge for Cyber-Physical Systems, led at VSU; 24 earned certificates.
- 24 students trained through CyberDevOps (AWS Cloud/DevOps), a cross-institutional program enrolling 15 VCU and 9 VSU undergraduates; 8 earned the AWS Certified Cloud Practitioner credential.
- 14 students trained through CVN Drone Training and Certification, preparing for the FAA Part 107 Remote Pilot certificate. Participants came from UVA, the University of Richmond, and Reynolds Community College.

In total, 109 students completed CVN-supported training programs, earning 32 industry-recognized credentials, with a further 14 prepared for federal certification.

5.3.3 NoVA Node

Student Internships and Assistantships

- Graduate Research Assistants: 5
- Undergraduate Research Assistants: 66

- Graduate Assistants: 6 (CATAPULT and ASCEND programs)
- Undergraduate Assistants: 2 (CATAPULT and ASCEND programs)
- Internships: 87
- Project Teams: 4 Teams consisting of 4 graduate students, 11 undergraduate students, 19 career transitioners.
- High School Students: 50

Patents and Disclosures

8 patents granted

- “Attack Detection and Countermeasures for Autonomous Navigation,” Md Tanvir Arafin, Kevin Kornegay (US 12,438,890 B2).
- “Hyperspectral imaging of biofluids for biometric applications,” Emanuela Marasco (US 12,664,658 B2).
- “Strengthening integrity assurances for DNS data,” Burton S. Kaliski Jr., Eric Osterweil (US 12,388,840 B2).
- “Externally applying internal network domain name system (DNS) policies,” Michael Kaczmarek, Eric Osterweil (US 12,375,441 B1).
- “Systems and methods for gait-based user authentication for lightweight resource-constrained wearable devices,” Sai Manoj Pudukotai Dinakarrao, Pavlos Zouridakis (US 12,468,794 B2).
- “Federated graph neural network for fast anomaly detection in controller area networks,” Hengrun Zhang, Kai Zeng (US 12,488,049 B2).
- “Countering autonomous vehicle usage for ramming attacks,” Duminda Wijesekera, Santos Jha, Cing-Dao Kan, Zoran Duric, Fernando Camelli (US 12,646,406 B2).
- “Multi-access edge computing for roadside units,” Santos Jha, Suminda Wijesekera, Satish Koli, Mahbubul Alam Palash (US 12,658,035 B2).

5.3.4 SWVA Node

CCI SWVA seeks to promote correlated economic outcomes associated with its investment and support. These outcomes, such as entrepreneur support, jobs created, capital investment, and “other,” can be less well-defined than the immediate, quantifiable outputs associated with CCI’s seed investments, but nevertheless help advance the desired outcome of promoting Virginia and its regions as centers of cybersecurity excellence.

- **Industry buy-in to meet SWVA regional cybersecurity needs:** Following engagement with regional business leaders at the panel discussion at UVA’s College at Wise, CCI researchers partnered with industry contacts at CGI Federal to submit a proposal to the EDA. This proposal, Development and Innovation to Propel Advanced Manufacturing (DIPAM), is being revised upon recommendation from the EDA program manager and speaks to a large potential investment realized thanks to the efforts of CCI SWVA and its member institutions, as well as partial cost matching offered by CCI SWVA utilizing refunds from prior years’ fiscal allocations and unspent research programming funding. In addition to this proposal collaboration, CCI SWVA has partnered with CGI Federal to offer two internships to scale programming and engage students in economically disadvantaged sectors of the region.

- **Region-specific promotion of nontraditional cybersecurity career pathways:** SWVA has a rich history rooted in the agricultural and mining industries; historically, workforce development has focused on industries other than cybersecurity. By seeking to engage local and regional economic development agencies as well as their industry collaborators, CCI SWVA has pivoted in FY26 towards a greater emphasis on supporting internships at regional businesses and municipalities to mirror the reality expressed by companies in our region that cybersecurity jobs in SWVA often arise at organizations that are not devoted exclusively to cybersecurity or as supplemental duties beyond a baseline job description. Examples of new experiential learning in FY26 include positions at regional grocery distributor Food City (KVAT, Inc.), municipal government agencies such as Roanoke City Public Schools, and startups such as the Music Advocacy Project. CCI SWVA subsidized a total of 72 interns in FY26, a 35% increase from FY25's 53 interns. In partnership with the InternshipsVA program established by Virginia Economic Development Partnerships (VEDP), CCI SWVA seeks to further grow and promote this program in the coming year. Early efforts are underway to promote this program in connection with the incoming Google Data Center, which is scheduled to break ground in Botetourt County later this year. By leveraging Google's historic multi-billion-dollar investment in the county and surrounding region, SWVA can embrace the potential of new industries while acknowledging its rich history.
- **Researchers explored the potential for technology translation and commercialization:** All recipients of research funding from CCI SWVA must "participate in an initial exploratory meeting with a representative from LINK+LICENSE+LAUNCH, a mentor from the Innovation Commercialization Assistance (ICAP) program, or personnel at a similar unit within the PI's institution within the first quarter of project performance. The goal of this initial meeting is to assess viability and/or interest in the potential commercialization of research deliverables." As in prior years, CCI SWVA saw broad compliance with this requirement; from the 27 grants issued in FY26, and seventeen (17) faculty members have already met with a commercialization office at their respective institution to evaluate commercial potential for their technology (awardees may meet at any time during the proposed work, resulting in some FY26 awardees opting to meet next year to give time for the technology to mature). Of the 17 meetings, nine (9) teams are proceeding with the office to formally establish intellectual property (IP) agreements.
- **2025 CCI IMPACT Award-Winning Professional Accelerated Cyber Education (PACE):** The PACE program at Radford University exceeded its original workforce development objectives by expanding cybersecurity training opportunities across SWVA and demonstrating sustained employer demand for flexible, competency-based education. Through the original CCI-funded project, 62 professionals enrolled in CBIT101, an online, self-paced cybersecurity course. The FY26 continuation award built upon this foundation by supporting participant progression into the full cybersecurity certificate pathway, aligned with industry-recognized credentials such as CompTIA Security+, CEH, and SANS GIAC GPEN. Beyond direct training outcomes, the project increased engagement with regional employers, local governments, and educational organizations, including the City of Winchester, Roanoke County, Prince William County Public Schools, the Town of Abingdon, and Modea. These partnerships validated the need for accessible cybersecurity workforce development and strengthened relationships that can support future enrollment growth and program sustainability. The project also contributed to regional workforce and economic development through presentations and stakeholder engagement activities, including the Region 7 CTE Directors Meeting, the Onward NRV Spring Leaders' Summit, and the TechIT Summit. These activities expanded awareness of cybersecurity career pathways, competency-based education, and workforce upskilling opportunities throughout the region. Finally, the success of PACE has strengthened Radford University's position to pursue future workforce development opportunities and grants that build on this model, helping establish a sustainable pipeline for cybersecurity talent development in SWVA.
- **Research Program Participation for Students:** In FY26, CCI SWVA directly supported 74 graduate students and 41 undergraduate students, as reported by principal investigators, on active research programs. These graduate and undergraduate students had the opportunity to work with experienced faculty members on funded research, learning the skills needed to prepare them for cybersecurity careers.

Chapter 6

Financial Report

6.1 CCI Hub

The budget and expenditures for the CCI Hub in FY26 are in Appendix 4.

CCI remained focused on its three mission areas, Research, Innovation, and Workforce Development, throughout FY26. CCI researchers and students conducted cutting-edge cybersecurity research, while workforce development and innovation programs expanded to reach more students and entrepreneurs across the commonwealth. Additionally, CCI built upon and publicized the positive findings from the third Economic Impact Study completed in FY25.

Operations continued to support the CCI mission and the research and innovation communities throughout the state. CCI successfully hosted the annual CCI Symposium in Richmond, Virginia, and welcomed international delegations and industry and government partners to the VT Research Center–Arlington (VTRC-A) to foster collaboration and strengthen Virginia’s cybersecurity ecosystem. CCI initiated planning to renovate the xG Testbed to improve its functionality and add presentation space, enabling the center to host visitors and conduct research demonstrations within the testbed. During FY26, CCI fully implemented a digital research technical reporting system through the America Learns Impact Suite. The digital reporting platform established a standardized data collection process that improved analysis, reporting, and program assessment.

Communications and marketing played a significant role in advertising, promoting, documenting, and branding the many CCI-sponsored, co-sponsored, and attended events throughout FY26. CCI updated and enhanced its website while continuing to leverage social media platforms and expand its digital presence to promote events, highlight researchers, and showcase the positive impacts of cybersecurity research, workforce development, and innovation across the commonwealth.

CCI continued to sponsor experiential learning programs, entrepreneurial incubators, and Cyber Fusion 2026. The CCI Hub partnered with regional companies to launch a statewide mentoring program to better prepare students to enter Virginia’s workforce. The Hub also increased the number of partner companies participating in the Project-Based Learning program, providing Virginia students with valuable real-world experience through industry collaborations. The CCI Hub continued to support the CATAPULT and ASCEND programs, which helped transition commercially viable research outcomes to the marketplace by providing education, marketing support, legal guidance, and mentoring from partner venture capital firms. In addition, the CCI Hub and the Regional Nodes collected workforce metrics and submitted them to Virginia Works as part of a Department of Labor initiative.

Throughout FY26, the xG Testbed continued to advance the nation’s first end-to-end O-RAN-compliant 5G/6G network with fully integrated AI infrastructure, while increasing utilization by researchers, students, and industry partners. Several large-scale collaborative projects with industry partners leveraged the xG Testbed for experimentation and testing. The CCI Hub also explored opportunities to monetize access to the xG Testbed for non-academic organizations seeking to utilize its unique capabilities.

CCI continued to sponsor cybersecurity research programs and supported multidisciplinary research addressing both the technical and human dimensions of cybersecurity, data, and autonomous systems. Researchers from institutions across the commonwealth continued to attract external funding by submitting

high-quality, collaborative proposals that produced high-impact results and further advanced Virginia's position as a global leader in cybersecurity innovation and research.

6.2 CCI Nodes

In FY26, 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 allocate funds to best meet the needs of its region and reinforce the cybersecurity research focus of its region's universities and verticals. In FY26, 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 CoVA Node

The budget and expenditures for the CoVA Node in FY26 are in Appendix 4.

The CoVA Center for Cyber Innovation, as part of the Commonwealth Cybersecurity Initiative, serves as the hub of southeastern Virginia for research, innovation, and commercialization of next-generation cybersecurity technologies, particularly in Cyber Physical Systems Security and Artificial Intelligence, across 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 CoVA Shared Academic and Research Environment. For ongoing funding of research scientists, resources have supported 12 faculty members hired at W&M, the ODU 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 CoVA 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 CoVA Center for Cyber Innovation.

6.2.2 CVN Node

The budget and expenditures for CVN in FY26 are provided in Appendix 4. During FY26, CVN committed \$990,000 in appropriated funds across three award lines: \$800,000 for research, \$100,000 for workforce development, and \$90,000 for commercialization. Operations funding supported regional staff, regional partnerships, and general operating expenses.

CVN maintained support for the testbeds available to the CCI network — Medical Device Security, Open-CyberCity, and NextG — which continue to serve as shared research infrastructure across the commonwealth. The node also brought a new shared computing resource into service: the CVN AI Testbed, comprising eight NVIDIA H100 GPUs, which entered operation in January 2026 and supported seven approved research projects in its first months, three of them tied directly to CVN -funded awards.

Research funding supported a node-wide call open to faculty across all CVN institutions. Eight projects were awarded at \$100,000 each, six of which are delivered by teams spanning two or more institutions, carrying subawards to VSU, Longwood University, and Piedmont Virginia Community College.

Regional funding opportunities for workforce development and commercialization were also supported. Two workforce development grants totaling \$100,000 were awarded, and three internal commercialization projects were funded at \$30,000 each through the Dreams to Reality Incubator at VCU. A further \$75,000 was allocated to the UVA to support internship placements, an AI training academy, student competitions, and a drone certification program.

CVN expanded its internship portfolio during the year, committing \$122,550 across four node-administered programs and launching Cyber Guardians, a new year-round placement program hosted within VCU Information Security.

6.2.3 NoVA Node

The budget and expenditures for the NoVA Node in FY26 are in Appendix 4.

In FY26, the CCI NoVA Node made significant investments in cybersecurity workforce development, addressing talent pipeline challenges through multiple entry points and innovative training and partnership approaches. The NoVA Node also strengthened Virginia's cybersecurity innovation ecosystem through the Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT) and Academic Support Cybersecurity Entrepreneurship and Next-Gen Development (ASCEND) funds, as well as continued investment in the CCI+A cybersecurity accelerator. These initiatives provided seed funding and comprehensive support services to cybersecurity startups, positioning them for long-term success while encouraging them to establish and grow within the commonwealth.

The NoVA Node's research investments further matured its research and development portfolio, directly supporting the cybersecurity innovation ecosystem and serving as a significant catalyst for attracting external research funding to strengthen Virginia's cybersecurity research enterprise.

Throughout the fiscal year, the NoVA Node cultivated a strategically integrated portfolio in which workforce development, research, and entrepreneurship reinforced one another. Workforce initiatives supported research activities and entrepreneurial success, while research investments were intentionally aligned with the expansion of the cybersecurity innovation ecosystem. This coordinated framework and demonstrated record of impact positioned the NoVA Node for continued growth and increased statewide impact.

CCI investments supported the NoVA Node's operational capacity by funding a full-time project manager to coordinate day-to-day programs and partnerships, as well as partial support for the NoVA Node Director's leadership and strategic oversight.

The NoVA Node's Living Innovation Laboratory infrastructure and associated faculty research enterprise matured significantly, creating a strong foundation for continued expansion. These investments enhanced the participating research universities' ability to compete for externally sponsored research, including federal funding, while expanding the commonwealth's cybersecurity research capabilities.

The NoVA Node continued to strengthen cybersecurity research infrastructure across its partner institutions as well and supported collaborative research aligned with the Node's priority areas, including national defense, critical infrastructure, transportation, electric power distribution, manufacturing, and the resilience of cyber systems to human behavior. The Node also expanded partnerships with industry and government organizations, increasing collaboration and support for its research portfolio.

Workforce development remained a central focus throughout FY26. The NoVA Node expanded experiential learning opportunities for high school, undergraduate, and graduate students, as well as individuals seeking to transition into cybersecurity careers. These programs enabled participants to apply classroom knowledge to real-world cybersecurity challenges while helping bridge the experience gap for employers. Investments also supported career readiness initiatives, including the Clearance Readiness Program, which prepared students to navigate the federal security clearance process and recognized their readiness through digital credentials that enhanced their visibility to employers.

Additional workforce investments expanded training opportunities for non-degree-seeking learners, with particular emphasis on career changers and individuals without prior cybersecurity experience, broadening the commonwealth's cybersecurity talent pipeline. The NoVA Node also expanded undergraduate internship opportunities with established and emerging technology companies and launched a pilot program that

embedded undergraduate teams, mentored by graduate students, within industry organizations to address real-world cybersecurity challenges.

The NoVA Node continued to strengthen NoVA’s and the commonwealth’s cybersecurity innovation and entrepreneurship ecosystem through sustained investments in the CATAPULT and ASCEND funds. These programs accelerated collaborative translational research projects among CCI partner institutions, helping move academic research toward commercialization while increasing collaboration between faculty and industry. Continued investment in the CCI+A cybersecurity accelerator built upon the program’s success since its launch in FY22, supporting cybersecurity startups through seed funding and comprehensive business development services. These efforts further expanded Virginia’s pipeline of high-growth cybersecurity companies and reinforced the commonwealth’s position as a national leader in cybersecurity innovation.

6.2.4 SWVA Node

The budget and expenditures for the SWVA Node in FY26 are in Appendix 4.

The CCI SWVA advances Virginia’s position as a global leader in secure cyber-physical systems by promoting cybersecurity research, innovation, and workforce development throughout SWVA. CCI SWVA partners with researchers who demonstrate technical excellence in cybersecurity, wireless communications, and emerging technologies, leveraging unique and expansive capabilities across application domains, including transportation, power systems, manufacturing, and agriculture. These collaborations support the discovery, demonstration, and commercialization of innovative technological solutions that contribute to the advancement of the cybersecurity state-of-the-art.

During the reporting period, CCI SWVA supported major research initiatives while building upon prior investments. CCI SWVA continued to provide funding for key research areas, including data security, communications, power and energy systems, transportation, and cyberbiosecurity. These investments advanced research programs in quantum communication, Artificial Intelligence (AI) assurance, 5G and next-G wireless systems and security, cryptography, system and software security, autonomous vehicle safety, and secure power grids. Funding also supported postdoctoral associates and professional development opportunities for graduate research assistants, strengthening the region’s research capacity and workforce.

CCI SWVA also advanced its mission to promote regional innovation by funding a competitive Innovation Call for Proposals to support the broader SWVA innovation ecosystem. Talent Pipeline initiatives included the CCI SWVA Internship Program, which engaged students from partner institutions and connected them with regional companies and startups. In addition, CCI SWVA supported student entrepreneurship programs that fostered innovation, commercialization, and the development of future technology leaders.

6.3 Geographic distribution of the awards from Appropriated Funds

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

Node	Number of Awards	Grant Total
Central Virginia	8	\$3,205,000
Coastal Virginia	13	\$3,566,000
Northern Virginia	7	\$3,315,000
Southwest Virginia	10	\$3,359,968
Total	38	\$13,445,968

Figure 6.1: Geographic distribution of awards from appropriated funds.

Chapter 7

Looking Ahead: FY27

In FY26, we continued to expand our research, innovation, and workforce development programs. An economic impact study conducted independently by RTI International revealed that CCI has thus far contributed over half a billion dollars to the Gross Domestic Product (GDP) of the commonwealth. While this report thus far has presented CCI's accomplishments in FY26, this final chapter outlines some of our areas of focus in FY27.

Focus area: AI Challenges to Cybersecurity

Each year, we invest in one or more key areas in cybersecurity, with the goal of building capacity that yields strong Return on Investment (RoI). This RoI manifests itself concretely in terms of funding that our researchers are able to attract from sources outside of the commonwealth. Our recent economic impact study estimates that for every \$1 that we invest in research seed grants, we obtain \$7 in research funding from the private sector and federal agencies.

In FY25, our key area of investment was AI for cybersecurity and cybersecurity for AI. In FY26, our major investment was in work to secure critical infrastructure against cyberattacks. In these past years, AI has become so closely linked to cybersecurity that virtually all work that is conducted by our researchers involves a combination of the two.

In FY27, we will focus our research investments on the new threats and challenges that AI is presenting to cybersecurity. AI is being used to generate highly personalized, and therefore more convincing, social engineering attacks. Recently, Anthropic's Mythos has shown the ability to reveal bugs and vulnerabilities not previously known in major browsers and open-source software. We are also seeing new attacks targeting AI systems, such as data poisoning, prompt injection, and data leakage. And, perhaps more than anything else, agentic AI is the new frontier in cybersecurity, with the recent Hugging Face incident as a major example of how powerful these systems can be.

This is a highly critical and timely topic for research. With the speed with which AI is moving, advances in this area can transition quickly into commercialization. Investing in this area brings potential return for all three of our mission lines of research, innovation, and workforce development.

We are launching a major program in Fall 2026, with the following objectives:

- To produce seminal contributions to the field of AI-generated cyber vulnerabilities, targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources.
- To contribute to the development of a skilled workforce with strong domain knowledge in both AI and cybersecurity.
- To produce research contributions that translate into benefits to Virginia companies.
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) in critical infrastructure cybersecurity.

Continuing to Expand our Innovation Programs

In FY26, our flagship innovation programs, CATAPULT and ASCEND, jointly run and funded by CCI's NoVA Node and the CCI Hub, have funded a record number of teams towards the commercialization of cybersecurity innovation created by the CCI network. Since their inception, these programs have continually evolved to effectively bring new ideas to commercialization. The CCI Hub and Node teams are currently planning for the FY27 version of the call for funding.

The CCI Hub is also bringing on board a Director of Outreach, who will be tasked with expanding this and other innovation programs open to the entire CCI network.

Building Teams to Compete for Large-scale Grants

One characteristic of the federally funded research landscape is an increased focus on large-scale challenges that require multi-institution and industry collaboration. In addition, solicitations from government agencies often require an accelerated response time. To respond effectively to these opportunities, it is important that the teams and networks be in place in advance of the publication of the call for proposals.

To this end, CCI will create a program that will fund the establishment of large, multi-university teams targeting large grants. The selection of these teams will be done through an open, peer-reviewed call for proposals. The final deliverable will be a proposal that is ready for submission to an appropriate funding program at the federal level or in the private sector. CCI will assemble a group of experts to red team the proposal and provide feedback to the authors. The goal is to anticipate areas of need in cybersecurity and be ready to respond quickly with an expert team of CCI researchers working with industry partners.

Continuous Improvement and Expansion of our Workforce Development Programs

The job market for cybersecurity talent remains as strong as ever. However, paradoxically, even entry-level jobs come with the expectation of substantial work experience. 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 FY27, we will continue to expand these programs through additional partnerships with Virginia companies of all sizes and state and federal agencies.

Convening the Virginia Cyber Community

Our annual symposium has reached record participation in FY26, with 290 researchers and students in attendance in Richmond, VA, in April. In 2027, we are moving the symposium to Charlottesville, VA, hosted by UVA.

We are also working with VIPC and an industry partner on convening a group of 40 to 50 experts in an invitation-only event focusing on the intersection of cybersecurity and quantum information sciences and technology. Objectives include producing a roadmap for Virginia's assets and investments in this area, as well as identifying opportunities for research and workforce development funding in this important growth area.

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 FY27, 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 FY26

Appendix 2: CCI Critical Infrastructure Cybersecurity Research Grants FY26

Appendix 3: Node Research Grants FY26

Appendix 4: FY26 Financial Reports

Appendix 1: CCI Extramural Funding for FY26

CCI Hub

Project Title	Institution	Funding Amount	Funding Agency
Secure 5G Side link - Air-Gapped 5G Connectivity	Virginia Tech	\$3,280	Cape
LDRD Full Proposal: Conflict Mitigation in Disaggregated Wireless Networks	Virginia Tech	\$179,772	Battelle Energy Alliance
IUCRC Phase 1 George Mason University: Center for Wireless Innovation towards Secure, Pervasive, Efficient, and Resilient Next G Networks (WISPER)	Virginia Tech	\$20,000	NSF
IUCRC Phase I Virginia Tech: Center for Wireless Innovation towards Secure, Pervasive, Efficient, and Resilient Next G Networks (WISPER)	Virginia Tech	\$150,000	NSF
NOFO-2 SFRA-1 Support to Abside	Virginia Tech	\$1,161,613	Abside Networks
Enhancing O-RAN Systems Against Sophisticated Attacks	Virginia Tech	\$92,614	Booz Allen Hamilton
Planning: Accelerating Innovation in Distributed AI Applications using an Open Radio Access Network (O-RAN) Testbed	Virginia Tech	\$90,011	NSF
Collaborative Research: A Novel Architecture for Secure and Adaptive Spectrum Management Enabling Registration-Free Federal Users	Virginia Tech	\$100,266	NSF
RAN Slicing Framework for Networked	Virginia Tech	\$154,542	WISPER

Project Title	Institution	Funding Amount	Funding Agency
IUCRC Phase 1 University of Arizona: Center for Wireless Innovation towards Secure, Pervasive, Efficient, and Resilient Next G Networks (WISPER)	Virginia Tech	\$20,000	NSF
Byzantine Resilient Federated Learning in Sporadically Connected Wireless Networks (PI: Wenjing Lou)	Virginia Tech	\$27,419	ONR
NITRD/WSRD Spectrum Workshop 2026	Virginia Tech	\$19,467	NSF
Research on Japan-US communication technology strategy	Virginia Tech	\$160,000	Washington Core
Research on the cybersecurity ecosystem in US and Japan	Virginia Tech	\$144,000	Kuwadate Inc
SCOPE (Software-Only Capacity Optimization & Performance Evaluation)	Virginia Tech	\$63,840	ANSpect Technologies LLC
Transformer-based Inter- Cell Coordination/MU- MIMO on OCUDU	Virginia Tech	\$892,211	Softbank Corp
2025-2026 Cyber SMART Projects	Virginia Tech	\$377,392	Georgetown University
Total		\$3,656,429	

Central Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
SPIRAL Phase II STTR	University of Virginia	\$425,000	Army Research Laboratory
CyberAI Innovation: Preparing AI-Native Software Engineers for Secure Software Development (Award 2622911)	Virginia Commonwealth University	\$250,000	NSF
LS2M: Towards Large Spatial Spectrum Model for Beam Management in 6G	University of Virginia	\$100,000	NVIDIA Academic Grant Program
Genetic Architecture of Neurodevelopmental Disorders: A Pilot Study Integrating Biobank-Scale Sequencing, Phenotypic Data, and Deep Learning Analysis (Dinh: Co-PI)	Virginia Commonwealth University	\$50,000	Children's Health Research Institute
CyberAI Innovation: Teaching Adversarial Causal Reasoning for AI-Augmented Security Operations	University of Virginia	\$500,000	NSF
An Integrated 2D and 3D Graph Machine Learning Platform for Peptide Discovery	University of Virginia	\$815,002	NSF
CAREER: Advancing Differentially Private Data Synthesis (Award 2543284)	University of Virginia	\$677,866	NSF
LLM Embodiment for Collaborative Autonomy	University of Virginia	\$500,000	DARPA
Convergence Lab Initiative (CLI)	Virginia Commonwealth University	\$2,600,000	DoW
Total		\$5,917,868	

Coastal Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
Machine Learning Empowered O-RAN based Dynamic Spectrum Management	ODU	\$4,189,723	CACI
Enhancing Joint Live, Virtual, and Constructive (JLVC) Training Environment	ODU	\$2,319,948	DoW/Systems Engineering Research Center
SCC-IRG: Resilient Sheltering Decision Support for Emergency Evacuations using Explainable AI	ODU	\$1,250,000	NSF
Applying AI/ML to Forecast Community Health Needs and Plan Public/Private Resource Allocation to Mitigate the Impacts of Stricter FY26 Medicaid Eligibility Rules	ODU	\$612,500	HIH
Department of Defense Cyber Service Academy (DoD CSA) Program at Old Dominion University	ODU	\$465,027	DoW
CRII: CNS: Secure Decentralized AI in Heterogeneous IoT Networks: Foundation and Application	ODU	\$145,830	NSF
IRAD Automated Threat Modeling for Agentic AI Systems	ODU	\$82,000	OERI
COVACoConnectAI: Leading Coastal Virginia in AI	ODU	\$75,000	SCHEV
Empirical Evaluation and Open-Source Enablement of Low-Latency Networking: L4S and NQB Queuing Architectures for Improved End-User Quality	CNU	\$60,000	COMCAST
Quantitative Assessment of Hybrid Infrastructure for AI-Enabled, Multi-Disciplinary Coastal Resilience under Recurring Tidal Flooding	ODU	\$31,000	CARMA
A Knowledge-Guided Multitask LLM for Software Vulnerability Detection, Reasoning, and Mitigation	W&M	\$25,000	NSF

Project Title	Institution	Funding Amount	Funding Agency
Flight Lab: Fundamentals of Drone Coding	CNU	\$15,277	VIVA
Generating hyper-Local Ecosystem and Terrain Datasets using Modified Low-Cost UAS Platforms to Support Applied Geospatial Research	CNU	\$1,250	Virginia Academy of Science
Total		\$9,272,555	

Northern Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
DoW Cyber Service Academy	George Mason University	\$250,000	DoW
DoW Cyber Service Academy	George Mason University	\$25,938	DoW
Artificial Intelligence, Cybersecurity, Industry Collaboration	George Mason University	\$25,000	New Push
CyberSTAR: Cyber Training for Secure Transportation and Reliable Autonomy	George Mason University	\$144,000	NSF
CyberSTAR: Cyber Training for Secure Transportation and Reliable Autonomy	George Mason University	\$56,000	NSF
Secure Accelerators for Next-Generation Foundation Models	George Mason University	\$275,000	NSF
HAYSTACK	George Mason University	\$9,093	IAPRA
Privacy Preserving Transactions with Accountability Extensions	George Mason University	\$226,508	NSF
Forged Insights	George Mason University	\$165,808	DoW
Extracting High Resolution Harmonic Fingerprinting from Sparse Sampling to Disaggregate Complex CVDs	George Mason University	\$200,000	ONR
Persistent Airborne Counter UAS Surveillance	George Mason University	\$69,904	Navy

Project Title	Institution	Funding Amount	Funding Agency
Quick Look Study of US Marine Corps Wargaming and Analysis Capability with Recommendations	George Mason University	\$98,500	DoW
Architecture and Workforce Development for Energy Centric UAS Research, Innovation, and Training for Critical Infrastructure Applications	George Mason University	\$100,000	CCALS
Unified Secure Research and Development Environment for Ground Vehicle Systems Center (GVSC)	George Mason University	\$599,996	Army
Virtual Prototyping of Mission and Formation Concepts with Autonomy Enabled Ground and Air Systems	George Mason University	\$303,886	Army
ISaC Workshop 2	George Mason University	\$293,802	AFRL
ISaC Workshop 2	George Mason University	\$5,000	AFRL
ISaC Workshop 3	George Mason University	\$154,874	AFRL
Synthesizing Temporal Logic and Human Performance Models for Deception Mitigation	George Mason University	\$549,107	ONR
Autonomy Standards and Ideals with Military Operational Values (ASIMOV)	George Mason University	\$101,791	DARPA

Project Title	Institution	Funding Amount	Funding Agency
VidStream	George Mason University	\$203,219	NSF
CoMIC: Collaborative Mobile Immersive Computing)	George Mason University	\$16,000	NSF
Scaling up Multi-user Immersive Content Delivery over mmWave	George Mason University	\$540,000	NSF
Revolutionizing Immersive Video Streaming with Neural Content Representation	George Mason University	\$275,000	NSF
OpenCIVAN: Scoping and Planning for an Open-Source Ecosystem for Collaborative and Immersive Visualization and Analytics in a Networked Environment	George Mason University	\$320,000	NSF
Mach-Q: Modular and Error-Aware Software Stack for Heterogeneous Quantum Computing Ecosystems	George Mason University	\$40,000	DoE
Quantum System Stability and Reproducibility Workshop	George Mason University	\$15,000	NSF
QuAIM: A Quantum Cyberinfrastructure with Automated Implementation Toolkits for Scientific Discovery	George Mason University	\$380,000	NSF
SPV: Synthesizing, Profiling, and Verification of Quantum Circuits	George Mason University	\$250,000	NSF

Project Title	Institution	Funding Amount	Funding Agency
Scammed by Love: Toward Mitigating AI-Facilitated Romance Scams Against Older Adults through Empirical	George Mason University	\$100,000	Google
SDR Analysis	George Mason University	\$37,630	DoW
Vehicle Network Security Architecture for Next-Generation Military Ground Vehicle Active	George Mason University	\$499,364	Army
SDR: Time Series Analysis	George Mason University	\$59,247	VECTARE/DoW
AFCENT CEC Applied Research 3	George Mason University	\$1,979,958	AFRL
AFCENT CEC Applied Research 3	George Mason University	\$62,735	AFRL
AFCENT CEC Applied Research	George Mason University	\$1,718,000	AFRL
AFCENT CEC Applied Research	George Mason University	\$500,000	AFRL
AFCENT Applied Research	George Mason University	\$750,000	AFRL
AFCENT Applied Research	George Mason University	\$400,000	AFRL
AFCENT Applied Research	George Mason University	\$800,000	AFRL
Crime Scene Surveying for IoT Investigations	George Mason University	\$88,272	DoJ
Accelerator Design Research	George Mason University	\$103,503	NSF
WISPER: Center for Wireless Innovation towards Secure, Pervasive, and Resilient Next G Networks	George Mason University	\$149,999	NSF

Project Title	Institution	Funding Amount	Funding Agency
Spectrum Sharing	George Mason University	\$50,000	NSF
Evaluation: Housing First Support Services	George Mason University	\$113,621	FFC
A Programmable Processor-in-Memory Accelerator for Data-Intensive and Deep Learning	George Mason University	\$115,791	DHL/NSF
CogFuzz: Cognitive and Design-aware Scalable Golden Reference Model (GRM)-free Hardware Fuzzing	George Mason University	\$125,000	ONR
SCC-IRG: Resilient Sheltering Decision Support for Emergency Evacuations using Explainable AI	George Mason University	\$1,250,000	NSF
MEADOW: Management Environment and Algorithms for Distributed Optimal Workflows	George Mason University	\$212,500	AFRL
Integrated Photonics for Sustained Operations - Phase III	George Mason University	\$296,998	NCMS/DoW
MARAAI: Mission Assurance Reference Architecture for Autonomy Integration Command and Control Systems	George Mason University	\$55,000	Bernd Group
Reference-based Automatic Security Patch Generation	George Mason University	\$69,266	ONR
EAGLE: Empowering American Government Leadership in Cybersecurity through Education	George Mason University	\$272,334	NSF
EAGLE: Empowering American Government Leadership in Cybersecurity through Education	George Mason University	\$768,651	NSF

Project Title	Institution	Funding Amount	Funding Agency
An Infrastructure and Dataset for Research in Software Vulnerability Detection and Remediation	George Mason University	\$45,000	NSF
Literacy Prototype	George Mason University	\$274,000	CDAO
Literacy Prototype	George Mason University	\$16,755	CDAO
Literacy Prototype	George Mason University	\$65,000	CDAO
ARCHER Integration	George Mason University	\$70,000	FHWA
SENTINEL: Side-channel Evaluation & Novel Techniques in XSOC	George Mason University	\$50,000	XSOC Corp
Operational Technology Digital Twin and Scanning Support	George Mason University	\$50,000	Datalytica
Vision-Language-Action Models for Off-Road Integrated Teams	George Mason University	\$517,604	Army
Hasty Defense with Attrition in Integrated Manned-Unmanned Formations	George Mason University	\$513,248	Army
Study Coordinated Human Eye Motion and Strabismus Using a Novel Artificial Muscle-Driven Robotic Eyes	George Mason University	\$587,450	NIH
Natural EXTension (NEXT)	George Mason University	\$243,771	ONR
A Unified Event-triggered Real-Time Scheduling and Control Co-Design Framework for Networked Safety-critical Control Systems	George Mason University	\$628,260	NSF
SourceCode	George Mason University	\$211,419	NSF

Project Title	Institution	Funding Amount	Funding Agency
Agentic Mechanistic Interpretation of Language Models	George Mason University	\$100,000	Foresight Institute
BRIDGE: Bridging Redundant Information for Data Governance and Efficiency	George Mason University	\$77,000	Naval Sea Systems Command
SECURIS: Securing Next G Millimeter-Wave Communication in Programmable RF Environments with Reconfigurable Intelligent Surface	George Mason University	\$254,745	NSF
Detection Tools in Smart Contracts	George Mason University	\$30,000	NSF
A Novel Performance Profiling and Analysis Infrastructure for Scientific Deep Learning	George Mason University	\$274,265	NSF
Harnessing Interpretable Neuro-Symbolic Learning for Reliable Ranking	George Mason University	\$599,635	NSF
Total		\$20,879,447	

Southwest Virginia Node

Project Title	Institution	Funding Amount	Funding Agency
Stochastic Optimization and ML Approaches for Interdependent Networked Systems: Applications for Water Distribution Systems	Virginia Tech	\$35,000	4-VA
Reward Design for Foundation Model Safety and Reasoning	Virginia Tech	\$72,500	Amazon
Travel Grant	Virginia Tech	\$2,300	AWM
Exhibit: Collection, Reframed: We Are Here, Beyond Vision	Virginia Tech	\$20,000	Bechtler Museum of Modern Art
VideoGym: Verifiable Video Understanding with Tool-Augmented Reasoning and Online Reinforcement Learning	Virginia Tech	\$75,000	Cisco
Virginia Tech IT Security Office and Lab (ITSO)	Virginia Tech	\$5,000	Commonwealth of Virginia
QuSen: Sub-threshold defect formation and its impact on phonon energy reconstruction	Virginia Tech	\$609,000	DARPA
COMPASS: Intrinsic Information in Spatial Fields: A Stochastic Geometry Approach to Spatial Inference	Virginia Tech	\$300,000	DARPA
COMPASS: Beyond Fisher: Novel Curvature-Based Accuracy Bounds for Resilient Signals-of-Opportunity-Based Localization	Virginia Tech	\$300,000	DARPA
"Exploring the feasibility of recoilless resonant neutrino absorption"	Virginia Tech	\$414,000	DOE
CLIN 0201	Virginia Tech	\$224,054	Federal (Restricted)
CLIN 0301	Virginia Tech	\$333,496	Federal (Restricted)
Towards Safe and Robust Agentic AI for the Open Web	Virginia Tech	\$60,000	Google
Securing Telco Ecosystems Against AI-Empowered Spam and Bot Attacks	Virginia Tech	\$485,373	GSMA
Visualizing LLM Feature Explanation in Analyst Workflows	Virginia Tech	\$15,892	NSA

Project Title	Institution	Funding Amount	Funding Agency
MORE: Mathematics – Opportunities in Research and Education	Virginia Tech	\$29,840	NSA
Randomized Sketching and Tensor-Format Solvers for High-Dimensional Models	Virginia Tech	\$249,581	NSF
CICI: IPAAI: A Traceable, Cost-Aware, and End-to-End Data Curation Framework for Medical AI	Virginia Tech	\$899,998	NSF
Collaborative Research: PDaSP: Track 2: Explainable Auditing of ML Models for Privacy Violations	Virginia Tech	\$400,000	NSF
Coding for storage, computing, and quantum error correction	Virginia Tech	\$300,000	NSF
DRL: Student Understanding of Linear Algebra across Quantum Information Science	Virginia Tech	\$499,502	NSF
Collaborative Research: A Novel Architecture for Secure and Adaptive Spectrum Management Enabling Registration-Free Federal Users	Virginia Tech	\$522,499	NSF
ExLENT: Beginnings: Growing the Undergraduate Spectrum Workshop into an Undergraduate Spectrum Workforce Development Program	Virginia Tech	\$150,000	NSF
SaTC: CORE: Medium: Practical Generative AI to Enhance Security Classifiers by Overcoming Data Challenges	Virginia Tech	\$320,000	NSF
CAREER: Learning Quantum States: Robustness, Noise, and Novel Algorithms	Virginia Tech	\$721,412	NSF
CAREER: Perceptual Modeling for Deceptive Patterns in Immersive Virtual Environments	Virginia Tech	\$672,132	NSF
CAREER: Automated, Quality, and Trustworthy Scientific Information Extraction from Massive Text Data	Virginia Tech	\$400,000	NSF
Collaborative Research: SaTC 2.0: RES: Post-Quantum Cryptographic Protocols with Advanced Functionalities	Virginia Tech	\$600,000	NSF
Federal Funding (non-SBIR/STTR): Tokay Systems LLC - Developing secure communications for the industrial IoT	Virginia Tech	\$350,000	NSWC Dahlgren // Joint Intermediate Force Capabilities Office

Project Title	Institution	Funding Amount	Funding Agency
HATS-Fedora	Virginia Tech	\$208,000	Restricted
Proof-of-concept Prototype of Optical Multi-sensor for Automotive Electronics Applications	Virginia Tech	\$70,000	Toyota Research Institute North America
Multi-die Optical-Power Electronics Integration (MOPEN)	Virginia Tech	\$50,000	Toyota Research Institute North America
EMI-Impact Evaluation of Optical Gate-Driver	Virginia Tech	\$120,000	Toyota Research Institute North America
Development of Rapid and Accurate Detection and Diagnosis of <i>Neopestalotiopsis</i> Disease in Strawberry	Virginia Tech	\$51,740	Virginia Agricultural Council
Total		\$9,566,319	

Appendix 2: Critical Infrastructure Cybersecurity Research Grants

Coastal Virginia Node

Project Title	PI	Lead Institution	Grant Amount
OpenCIVI: Open Benchmarks and AI-Ready Defenses for Vehicle-to-Infrastructure	Sidi Lu	William & Mary	\$100,000
Intelligent Framework for Securing IoT Systems in Critical Infrastructure	Mahmoud Nazzal	Old Dominion University	\$100,000
Cyber-Resilient Multi-Sensor Radiation Monitoring for High-Energy Accelerators	Jiang Li	Old Dominion University	\$100,000
Autonomous LLM Agents for Microgrid SOC	Mohammad Ghasemigol	Old Dominion University	\$100,000
AI-Driven Security for Distributed Power-Grid: Integrated Layered Simulation and AI-Powered Attack/Defense Scenarios	Javad Rafiei Asl	Old Dominion University	\$100,000
SecureLFE: Securing LF Energy's Open-Source Ecosystem for Critical Energy Infrastructure	Yue Xiao	William & Mary	\$100,000

Central Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Bastion: Scalable Assurance for Critical Infrastructure through Generative Hardening and Robust Detection	Ashish Venkat	University of Virginia	\$100,000
SHIELD – Secure Hardware Infrastructure for Equipment Lifecycle Diagnostic	Mircea Stan	University of Virginia	\$100,000
FORTAI: AI-Enabled Zero-Trust Security Framework for Agentic AI Serving Infrastructures	Yue Cheng	University of Virginia	\$100,000
Quantum-AI Detection of Cyber-Physical Attacks on Smart Water Networks	Thang Dinh	Virginia Commonwealth University	\$100,000

Northern Virginia Node

Project Title	PI	Lead Institution	Grant Amount
AI-Powered Video and Audio Side Channels for Cyber-Physical Anomaly Detection in Critical Infrastructure	Lisa Luo	George Mason University	\$100,000
Scalable AI-driven Cybersecurity for Small and Medium Critical Manufacturing	Shima Mohebbi	George Mason University	\$100,000
Secure 6G Infrastructure for Integrated Sensing and Communication	Kai Zeng	George Mason University	\$100,000
CASPER: Cyber-Analog Sensing for Protecting Critical Energy Infrastructure	Md Tanvir Arafin	George Mason University	\$100,000
Explainable LSTM-Based Anomaly Detection for Operating Room HVAC and ICU Power Systems in Hospitals	Sanchari Das	George Mason University	\$100,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Grant Amount
LLM-Powered Intrusion Detection and Investigation in Modern Industrial Control Systems	Peng Gao	Virginia Tech	\$100,000
Securing NextG Networks via Context-aware Policy Enforcement	Bo Ji	Virginia Tech	\$100,000
Supporting Cyber Resilience of Energy Systems: Using AI to Enhance Malware Defenses in SCADA Systems	Onyeka Emebo	Virginia Tech	\$94,968
Z-TRACS: Zero-Trust Reinforcement Learning for Anti-Cyber Spoofing	Monty Abbas	Virginia Tech	\$100,000
Resilient Neuromorphic-NextG IoT Framework for Secure and Autonomous Water Infrastructure Cybersecurity	Cindy Yang Yi	Virginia Tech	\$100,000
Agentic AI for Scalable and Cost-Effective Protection of Critical Infrastructure	Murat Kantarcioglu	Virginia Tech	\$100,000

Appendix 3: CCI Node Research Programs for FY26

Central Virginia Node

FY26 Research Grants

Project Title	PI	Lead Institution	Grant Amount
Security Foundation for Cyber-Physical System Intelligence on Quantum Cloud	Thang N. Dinh	Virginia Commonwealth University	\$100,000
AI Meets the City: Real-World Deployment of Intelligent Systems	Sherif Abdelwahed; Milos Manic	Virginia Commonwealth University	\$100,000
Securing the Layered Build: Cyber-Physical Defense in Additive Manufacturing Systems of Metal Fused Filament Fabrication	R. Barua; Irfan Ahmed	Virginia Commonwealth University	\$100,000
Reinforced Sensory Intelligence for Safe Autonomous Driving	Shangtong Zhang	University of Virginia	\$100,000
Resilient and Adaptive Urban Transportation Routing for Emergency Management Services	Rohan Chandra; J. Goodall	University of Virginia	\$100,000
Foundations for Provenance-Based Security in AR/VR-Enabled Cyber-Physical Systems	Wajih Ul Hassan; H. Alemzadeh	University of Virginia	\$100,000
Resilient and Secure Cooperative Platooning for Automated Vehicles in Mixed Traffic	Brian Park	University of Virginia	\$100,000
Deception-Resilient Robot Security Monitoring	Nicola Bezzo	University of Virginia	\$100,000

Coastal Virginia Node

Agentic AI Cybersecurity and Security for Agentic AI

Project Title	PI	Lead Institution	Grant Amount
Securing Agentic AI Systems using Verified Behavioral Templates	P. Giabbanelli	Old Dominion University	\$80,000
Security and Privacy for Client-Hosted Agents via Trusted Hardware	J. Takeshita	Old Dominion University	\$80,000
Agentic AI for Multi-Modal Perception Integrity: Threat Reasoning and Response in Cyber-Physical Transportation Systems	Q. Ting	Old Dominion University	\$79,926
Securing Clustered Semantic Communications in Agentic AI Systems	L. Li	Old Dominion University	\$80,000
Enhancing Safety of Agentic AI for High- s Physical Systems	F. Liu	Old Dominion University	\$80,000
Securing Mobile Agentic AI Systems: Systematic Risk Analysis and Defense Against Confused Deputy Behavior	Y. Xiao	William & Mary	\$80,000

Northern Virginia Node

Research in Cybersecurity and Critical Infrastructure

Project Title	PI	Lead Institution	Grant Amount
Cyber Resilient Environments through Control Logic Aware Network Monitoring	Jared Stoltzfus	James Madison University	\$50,000
Agroforestry as Living Infrastructure: Applications and improvements of sensor networks in securing Virginia's farming livelihoods and improving sensor network security	Katherine Sinacore	James Madison University	\$50,000
AI-Powered Digital Twins for Cybersecurity of Critical Infrastructures	Hala Nelson	James Madison University	\$50,000
Enhancing Autonomous Transportation Systems Safety: Integrating AI and Cybersecurity for Real-Time Anomaly Detection	Samy El-Tawab	James Madison University	\$50,000
Persistent Threat Detection in Industrial Control Systems for Manufacturing Environments	Adeen Ayub	James Madison University	\$50,000

Research in Cybersecurity Supporting Industry-Faculty Collaboration

Project Title	PI	Lead Institution	Grant Amount
Building Capacity for Rapid Situational Awareness to Manage National Security Threats through a Resilient Emergency Communication Infrastructure with AI	Hemant Purohit	George Mason University	\$50,000
Secure Spectrum Analytics on the Edge using Deep Learning	Parth Pathak	George Mason University	\$50,000
Phase Space Physics Derived Modeling for Anomaly Detection in Manufacturing Systems	Matt Jablonski	George Mason University	\$50,000
Generative AI-enabled Linguistic Steganography for Covert and Resilient Communication	Kai Zeng	George Mason University	\$50,000

Southwest Virginia Node

FY26 Cybersecurity Research Program Grants

Project Title	Principal Investigator	Lead Institution	Grant Amount
Cybersecurity and Behavioral Risk Analytics in Remote Audit Practice: A Regional Study in Southwest Virginia and Appalachia	Gurkan Akalin	UVA College at Wise	\$60,000
Securing Embodied Systems Against Adversarial Audio Through Physical Acoustics	Alaa Algargoosh	Virginia Tech	\$59,984
Futureproofing Consensus Protocols for Blockchain and More: Constructing Quantum-Resistant Threshold (Ring) Signatures	Sarah Arpin	Virginia Tech	\$44,096
A Real-Time / Security Co-Scheduling Framework for Time-Sensitive, Zero-Trust CPS	Thidapat (Tam) Chantem	Virginia Tech	\$60,000
Quantum Change-point Detection: A Statistical Framework for Cyber-Physical Threat Recognition	Steven Flammia	Virginia Tech	\$58,888
Evolving Zero-Trust for O-RAN Defense: Interpretable and Verifiable AI for 5G NTN Fake Base Station Detection	Ming Jin	Virginia Tech	\$60,000
Supporting Military Family Cybersecurity with an AI-Infused OSINT Tool	Kurt Luther	Virginia Tech	\$59,815
Coding theory for modern secure communication and computation	Gretchen Matthews	Virginia Tech	\$60,000

Project Title	Principal Investigator	Lead Institution	Grant Amount
Data Privacy Landscape for Modern Transportation System While Using Multimodal Data	Abhijit Sarkar	Virginia Tech	\$60,000
Protecting AI with Security Guarantees using Confidential Virtual Machines with GPUs	Wenjie Xiong	Virginia Tech	\$60,000
RISE-IoT: Resilient Intelligent and Secured Edge IoT	Cindy Yang Yi	Virginia Tech	\$59,632

FY26 Research Engagement Program Grants

Project Title	PI	Lead Institution	Grant Amount
Cyber-Resilient Teen LLM Interactions: Preventing Privacy Leakage and Harm Escalation via Rewrite-Based Guardrails	Jin-Hee Cho	Virginia Tech	\$15,000
Quantum Error Corrected Networks with Logically Encoded Photonic States	Sophia Economou	Virginia Tech	\$15,000
Differential Fuzzing of Linkers and Loaders for Secure Software Toolchains	Peng Gao	Virginia Tech	\$15,000
AI-Augmented AR Interfaces for Space Cybersecurity: From Planning to Implementation	Christiana Chamon Garcia	Virginia Tech	\$15,000
ElasticFuzz: Flexible Distributed Fuzzing Infrastructure	Matthew Hicks	Virginia Tech	\$15,000
Cryptographic Foundations for Privacy-Preserving and Trustworthy Federated Learning	Thang Hoang	Virginia Tech	\$15,000
Undergraduate Summer Cybersecurity Research Internship	Hwajung Lee	Radford University	\$15,000
Energy-Efficient Sensing and Resilient Explainable AI for Smart Livestock Health Monitoring	Hwajung Lee et al.	Radford University	\$15,000
Efficient Tool-Gateway Enforcement and Behavioral Drift Detection for Secure LLM Agents	Na Meng	Virginia Tech	\$15,000
Autonomous Defensive Maneuvering for Cyber-Resilient Satellite Operations	Kevin Schroeder	Virginia Tech	\$15,000
Incentive-Compatible Federated Risk Detection for Cross-Institution Security Networks	Lecheng Zheng	Virginia Tech	\$14,999
AI Assurance for Safety-Critical Scenarios: Characterizing and Monitoring Hallucination Failures in Large Language Models	Dawei Zhou	Virginia Tech	\$15,000

Other Research Grants Awarded

Project Title	Principal Investigator	Lead Institution	Grant Amount
Cybersecurity Research Engagement	Gretchen Matthews	Virginia Tech	\$50,000
Security Scholar - Software Defined Radio and O-RAN for Mobile Distributed MIMO (dMIMO)	Lingjia Liu	Virginia Tech	\$49,522
Security Scholar - Graduate Research & Innovation Design: Secure Connectivity for Renewable Devices in the grid (GRID-SECURED)	Ali Mehrizi-Sani	Virginia Tech	\$49,431
Security Scholar - Task-based Model Selection	Hoda Eldardiry	Virginia Tech	\$49,552
Swissogeny Conference Support	Jason LeGrow	Virginia Tech	\$850
Steger Center Collaboration Workshop 2026	Gretchen Matthews	Virginia Tech	\$5,000
CCI SWVA Research Showcase 2026 - Travel Grant	Madison Boswell	Virginia Tech	\$764
CCI SWVA Research Showcase 2026 - Travel Grant	Peng Gao	Virginia Tech	\$312
CCI SWVA Research Showcase 2026 - Travel Grant	Abjit Sarkar	Virginia Tech	\$1,012
CCI SWVA Research Showcase 2026 - Travel Grant	Arianna Schuler Scott	Virginia Tech	\$489
CCI SWVA Research Showcase 2026 - Travel Grant	Gretchen Matthews	Virginia Tech	\$396
CCI SWVA Research Showcase 2026 - Travel Grant	Wenjie Xiong	Virginia Tech	\$600

Project Title	Principal Investigator	Lead Institution	Grant Amount
CCI SWVA Research Showcase 2026 - Travel Grant	Sarah Arpin	Virginia Tech	\$527
CCI SWVA Research Showcase 2026 - Travel Grant	Jason LeGrow	Virginia Tech	\$850
CCI SWVA Research Showcase 2026 - Travel Grant	Jai Kumar Sharma	Virginia Tech	\$470
CCI SWVA Research Showcase 2026 - Travel Grant	Chris Thomas	Virginia Tech	\$703
CCI SWVA Research Showcase 2026 – Travel Grant	Gurkan Akalin	UVA Wise	\$1,396
CCI SWVA Research Showcase 2026 – Travel Grant	Ning Zhou	UVA Wise	\$1,004

CCl Hub FY26 Finance Report

Line	Activity	4-2	4-3	4-4	4-5	4-6	4-7	4-8	4-9	4-10	4-11	4-12	4-13	4-14	4-15	4-16	4-17	4-18	4-19	4-20	4-21	4-22	4-23	4-24	4-25	4-26	4-27	4-28	4-29	4-30	4-31	4-32	4-33	4-34	4-35	4-36	4-37	4-38	4-39	4-40	4-41	4-42	4-43	4-44	4-45	4-46	4-47	4-48	4-49	4-50	4-51	4-52	4-53	4-54	4-55	4-56	4-57	4-58	4-59	4-60	4-61	4-62	4-63	4-64	4-65	4-66	4-67	4-68	4-69	4-70	4-71	4-72	4-73	4-74	4-75	4-76	4-77	4-78	4-79	4-80	4-81	4-82	4-83	4-84	4-85	4-86	4-87	4-88	4-89	4-90	4-91	4-92	4-93	4-94	4-95	4-96	4-97	4-98	4-99	4-100	4-101	4-102	4-103	4-104	4-105	4-106	4-107	4-108	4-109	4-110	4-111	4-112	4-113	4-114	4-115	4-116	4-117	4-118	4-119	4-120	4-121	4-122	4-123	4-124	4-125	4-126	4-127	4-128	4-129	4-130	4-131	4-132	4-133	4-134	4-135	4-136	4-137	4-138	4-139	4-140	4-141	4-142	4-143	4-144	4-145	4-146	4-147	4-148	4-149	4-150	4-151	4-152	4-153	4-154	4-155	4-156	4-157	4-158	4-159	4-160	4-161	4-162	4-163	4-164	4-165	4-166	4-167	4-168	4-169	4-170	4-171	4-172	4-173	4-174	4-175	4-176	4-177	4-178	4-179	4-180	4-181	4-182	4-183	4-184	4-185	4-186	4-187	4-188	4-189	4-190	4-191	4-192	4-193	4-194	4-195	4-196	4-197	4-198	4-199	4-200	4-201	4-202	4-203	4-204	4-205	4-206	4-207	4-208	4-209	4-210	4-211	4-212	4-213	4-214	4-215	4-216	4-217	4-218	4-219	4-220	4-221	4-222	4-223	4-224	4-225	4-226	4-227	4-228	4-229	4-230	4-231	4-232	4-233	4-234	4-235	4-236	4-237	4-238	4-239	4-240	4-241	4-242	4-243	4-244	4-245	4-246	4-247	4-248	4-249	4-250	4-251	4-252	4-253	4-254	4-255	4-256	4-257	4-258	4-259	4-260	4-261	4-262	4-263	4-264	4-265	4-266	4-267	4-268	4-269	4-270	4-271	4-272	4-273	4-274	4-275	4-276	4-277	4-278	4-279	4-280	4-281	4-282	4-283	4-284	4-285	4-286	4-287	4-288	4-289	4-290	4-291	4-292	4-293	4-294	4-295	4-296	4-297	4-298	4-299	4-300	4-301	4-302	4-303	4-304	4-305	4-306	4-307	4-308	4-309	4-310	4-311	4-312	4-313	4-314	4-315	4-316	4-317	4-318	4-319	4-320	4-321	4-322	4-323	4-324	4-325	4-326	4-327	4-328	4-329	4-330	4-331	4-332	4-333	4-334	4-335	4-336	4-337	4-338	4-339	4-340	4-341	4-342	4-343	4-344	4-345	4-346	4-347	4-348	4-349	4-350	4-351	4-352	4-353	4-354	4-355	4-356	4-357	4-358	4-359	4-360	4-361	4-362	4-363	4-364	4-365	4-366	4-367	4-368	4-369	4-370	4-371	4-372	4-373	4-374	4-375	4-376	4-377	4-378	4-379	4-380	4-381	4-382	4-383	4-384	4-385	4-386	4-387	4-388	4-389	4-390	4-391	4-392	4-393	4-394	4-395	4-396	4-397	4-398	4-399	4-400	4-401	4-402	4-403	4-404	4-405	4-406	4-407	4-408	4-409	4-410	4-411	4-412	4-413	4-414	4-415	4-416	4-417	4-418	4-419	4-420	4-421	4-422	4-423	4-424	4-425	4-426	4-427	4-428	4-429	4-430	4-431	4-432	4-433	4-434	4-435	4-436	4-437	4-438	4-439	4-440	4-441	4-442	4-443	4-444	4-445	4-446	4-447	4-448	4-449	4-450	4-451	4-452	4-453	4-454	4-455	4-456	4-457	4-458	4-459	4-460	4-461	4-462	4-463	4-464	4-465	4-466	4-467	4-468	4-469	4-470	4-471	4-472	4-473	4-474	4-475	4-476	4-477	4-478	4-479	4-480	4-481	4-482	4-483	4-484	4-485	4-486	4-487	4-488	4-489	4-490	4-491	4-492	4-493	4-494	4-495	4-496	4-497	4-498	4-499	4-500	4-501	4-502	4-503	4-504	4-505	4-506	4-507	4-508	4-509	4-510	4-511	4-512	4-513	4-514	4-515	4-516	4-517	4-518	4-519	4-520	4-521	4-522	4-523	4-524	4-525	4-526	4-527	4-528	4-529	4-530	4-531	4-532	4-533	4-534	4-535	4-536	4-537	4-538	4-539	4-540	4-541	4-542	4-543	4-544	4-545	4-546	4-547	4-548	4-549	4-550	4-551	4-552	4-553	4-554	4-555	4-556	4-557	4-558	4-559	4-560	4-561	4-562	4-563	4-564	4-565	4-566	4-567	4-568	4-569	4-570	4-571	4-572	4-573	4-574	4-575	4-576	4-577	4-578	4-579	4-580	4-581	4-582	4-583	4-584	4-585	4-586	4-587	4-588	4-589	4-590	4-591	4-592	4-593	4-594	4-595	4-596	4-597	4-598	4-599	4-600	4-601	4-602	4-603	4-604	4-605	4-606	4-607	4-608	4-609	4-610	4-611	4-612	4-613	4-614	4-615	4-616	4-617	4-618	4-619	4-620	4-621	4-622	4-623	4-624	4-625	4-626	4-627	4-628	4-629	4-630	4-631	4-632	4-633	4-634	4-635	4-636	4-637	4-638	4-639	4-640	4-641	4-642	4-643	4-644	4-645	4-646	4-647	4-648	4-649	4-650	4-651	4-652	4-653	4-654	4-655	4-656	4-657	4-658	4-659	4-660	4-661	4-662	4-663	4-664	4-665	4-666	4-667	4-668	4-669	4-670	4-671	4-672	4-673	4-674	4-675	4-676	4-677	4-678	4-679	4-680	4-681	4-682	4-683	4-684	4-685	4-686	4-687	4-688	4-689	4-690	4-691	4-692	4-693	4-694	4-695	4-696	4-697	4-698	4-699	4-700	4-701	4-702	4-703	4-704	4-705	4-706	4-707	4-708	4-709	4-710	4-711	4-712	4-713	4-714	4-715	4-716	4-717	4-718	4-719	4-720	4-721	4-722	4-723	4-724	4-725	4-726	4-727	4-728	4-729	4-730	4-731	4-732	4-733	4-734	4-735	4-736	4-737	4-738	4-739	4-740	4-741	4-742	4-743	4-744	4-745	4-746	4-747	4-748	4-749	4-750	4-751	4-752	4-753	4-754	4-755	4-756	4-757	4-758	4-759	4-760	4-761	4-762	4-763	4-764	4-765	4-766	4-767	4-768	4-769	4-770	4-771	4-772	4-773	4-774	4-775	4-776	4-777	4-778	4-779	4-780	4-781	4-782	4-783	4-784	4-785	4-786	4-787	4-788	4-789	4-790	4-791	4-792	4-793	4-794	4-795	4-796	4-797	4-798	4-799	4-800	4-801	4-802	4-803	4-804	4-805	4-806	4-807	4-808	4-809	4-810	4-811	4-812	4-813	4-814	4-815	4-816	4-817	4-818	4-819	4-820	4-821	4-822	4-823	4-824	4-825	4-826	4-827	4-828	4-829	4-830	4-831	4-832	4-833	4-834	4-835	4-836	4-837	4-838	4-839	4-840	4-841	4-842	4-843	4-844	4-845	4-846	4-847	4-848	4-849	4-850	4-851	4-852	4-853	4-854	4-855	4-856	4-857	4-858	4-859	4-860	4-861	4-862	4-863	4-864	4-865	4-866	4-867	4-868	4-869	4-870	4-871	4-872	4-873	4-874	4-875	4-876	4-877	4-878	4-879	4-880	4-881	4-882	4-883	4-884	4-885	4-886	4-887	4-888	4-889	4-890	4-891	4-892	4-893	4-894	4-895	4-896	4-897	4-898	4-899	4-900	4-901	4-902	4-903	4-904	4-905	4-906	4-907	4-908	4-909	4-910	4-911	4-912	4-913	4-914	4-915	4-916	4-917	4-918	4-919	4-920	4-921	4-922	4-923	4-924	4-925	4-926	4-927	4-928	4-929	4-930	4-931	4-932	4-933	4-934	4-935	4-936	4-937	4-938	4-939	4-940	4-941	4-942	4-943	4-944	4-945	4-946	4-947	4-948	4-949	4-950	4-951	4-952	4-953	4-954	4-955	4-956	4-957	4-958	4-959	4-960	4-961	4-962	4-963	4-964	4-965	4-966	4-967	4-968	4-969	4-970	4-971	4-972	4-973	4-974	4-975	4-976	4-977	4-978	4-979	4-980	4-981	4-982	4-983	4-984	4-985	4-986	4-987	4-988	4-989	4-990	4-991	4-992	4-993	4-994	4-995	4-996	4-997	4-998	4-999	500
1	500000 - 5000 -																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																							

Person / Category / Address (2000)	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030
Person A / Category A / Address A (2000)																																		
Person B / Category B / Address B (2000)																																		
Person C / Category C / Address C (2000)																																		
Person D / Category D / Address D (2000)																																		
Person E / Category E / Address E (2000)																																		
Person F / Category F / Address F (2000)																																		
Person G / Category G / Address G (2000)																																		
Person H / Category H / Address H (2000)																																		
Person I / Category I / Address I (2000)																																		
Person J / Category J / Address J (2000)																																		
Person K / Category K / Address K (2000)																																		
Person L / Category L / Address L (2000)																																		
Person M / Category M / Address M (2000)																																		
Person N / Category N / Address N (2000)																																		
Person O / Category O / Address O (2000)																																		
Person P / Category P / Address P (2000)																																		
Person Q / Category Q / Address Q (2000)																																		
Person R / Category R / Address R (2000)																																		
Person S / Category S / Address S (2000)																																		
Person T / Category T / Address T (2000)																																		
Person U / Category U / Address U (2000)																																		
Person V / Category V / Address V (2000)																																		
Person W / Category W / Address W (2000)																																		
Person X / Category X / Address X (2000)																																		
Person Y / Category Y / Address Y (2000)																																		
Person Z / Category Z / Address Z (2000)																																		
Person AA / Category AA / Address AA (2000)																																		
Person AB / Category AB / Address AB (2000)																																		
Person AC / Category AC / Address AC (2000)																																		
Person AD / Category AD / Address AD (2000)																																		
Person AE / Category AE / Address AE (2000)																																		
Person AF / Category AF / Address AF (2000)																																		
Person AG / Category AG / Address AG (2000)																																		
Person AH / Category AH / Address AH (2000)																																		
Person AI / Category AI / Address AI (2000)																																		
Person AJ / Category AJ / Address AJ (2000)																																		
Person AK / Category AK / Address AK (2000)																																		
Person AL / Category AL / Address AL (2000)																																		
Person AM / Category AM / Address AM (2000)																																		
Person AN / Category AN / Address AN (2000)																																		
Person AO / Category AO / Address AO (2000)																																		
Person AP / Category AP / Address AP (2000)																																		
Person AQ / Category AQ / Address AQ (2000)																																		
Person AR / Category AR / Address AR (2000)																																		
Person AS / Category AS / Address AS (2000)																																		
Person AT / Category AT / Address AT (2000)																																		
Person AU / Category AU / Address AU (2000)																																		
Person AV / Category AV / Address AV (2000)																																		
Person AW / Category AW / Address AW (2000)																																		
Person AX / Category AX / Address AX (2000)																																		
Person AY / Category AY / Address AY (2000)																																		
Person AZ / Category AZ / Address AZ (2000)																																		
Person BA / Category BA / Address BA (2000)																																		
Person BB / Category BB / Address BB (2000)																																		
Person BC / Category BC / Address BC (2000)																																		
Person BD / Category BD / Address BD (2000)																																		
Person BE / Category BE / Address BE (2000)																																		
Person BF / Category BF / Address BF (2000)																																		
Person BG / Category BG / Address BG (2000)																																		
Person BH / Category BH / Address BH (2000)																																		
Person BI / Category BI / Address BI (2000)																																		
Person BJ / Category BJ / Address BJ (2000)																																		
Person BK / Category BK / Address BK (2000)																																		
Person BL / Category BL / Address BL (2000)																																		
Person BM / Category BM / Address BM (2000)																																		
Person BN / Category BN / Address BN (2000)																																		
Person BO / Category BO / Address BO (2000)																																		
Person BP / Category BP / Address BP (2000)																																		
Person BQ / Category BQ / Address BQ (2000)																																		
Person BR / Category BR / Address BR (2000)																																		
Person BS / Category BS / Address BS (2000)																																		
Person BT / Category BT / Address BT (2000)																																		
Person BU / Category BU / Address BU (2000)																																		
Person BV / Category BV / Address BV (2000)																																		
Person BW / Category BW / Address BW (2000)																																		
Person BX / Category BX / Address BX (2000)																																		
Person BY / Category BY / Address BY (2000)																																		
Person BZ / Category BZ / Address BZ (2000)																																		
Person CA / Category CA / Address CA (2000)																																		

Total Spending and Encumbrance	Current FY Funds + Prior FY Carryover	%
		8,886,492

	12-25	Aug-25	Sept-25	Oct-25	Nov-25	Dec-25	Jan-26	Feb-26	Mar-26	Apr-26	May-26	Jun-26	Actual YTD	Revised YTD	YTD Encumbrance Budget
YTD Encumbrance Budget Available															
Toward Local Government, District & Federal, State & General Budget	\$ 2,432	1,826											\$ 2,736	\$ 334	\$ 1,172
ATI					\$ 48,848								\$ 88,848	\$ 8,852	\$ 32,568
Capitalized													-	192	162
Other encumbrance charge from YTD				742									\$ 742	\$ 742	-
YTD Encumbrance Budget Available	\$ 3,400	3,655	742	742	48,848								\$ 92,224	\$ 7,918	\$ 32,640

(remaining YTD encumbrance budget have been released)

All remaining P725 myocardial infarctions have been relevant.

Figure 1: CCI Hub FY26 Finance Report

	Jul-25	Aug-25	Sep-25	Oct-25	Nov-25	Dec-25	Jan-26	Feb-26	Mar-26	Apr-26	May-26	Jun-26	Actual YTD	FY26 Encumbered Funds	Budget Balance YTD	Budgeted
Burn Rate	0%	0%	0%	0%	0%	21%	21%	21%	21%	21%	21%	23%	23%			
Workforce Development & Commercialization																
WFD CFP	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 50,000	\$ -	\$ -	\$ -	\$ -	\$ 50,000	\$ -	\$ 100,000	\$ -	\$ -	\$ 150,000
Internships in CWN	\$ -	\$ -	\$ -	\$ -	\$ 4,800	\$ 75,200	\$ 1,800	\$ 1,200	\$ 600	\$ 1,200	\$ 1,200	\$ 2,240	\$ 33,540	\$ 122,880	\$ 54,120	\$ 27,120
Commercialization to VCU	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 90,000	\$ -	\$ -	\$ -	\$ -	\$ 60,000
Commercialization to UVA	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 60,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 60,000
CWN Partnerships	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 100,000
Subtotal	\$ -	\$ -	\$ -	\$ -	\$ 4,800	\$ 185,200	\$ 1,800	\$ 1,200	\$ 90,800	\$ 51,200	\$ 141,200	\$ 2,240	\$ 33,540	\$ 472,800	\$ 54,120	\$ 47,120
Burn Rate	0%	0%	0%	0%	1%	37%	37%	37%	47%	57%	84%	84%	91%	91%		
Research & Investment																
Support Existing Programs	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 150,000	\$ -	\$ 2,857	\$ 2,160	\$ 1,950	\$ 1,109	\$ 4,720	\$ 166,247	\$ -	\$ 88,596	\$ 450,000
Research Facility	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 125,000
Research CFPs	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 700,000	\$ 100,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 800,000	\$ -	\$ -
Subtotal	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 850,000	\$ 100,000	\$ 2,857	\$ 2,160	\$ 1,950	\$ 1,109	\$ 4,720	\$ 166,247	\$ 1,129,063	\$ 88,596	\$ 245,937
Burn Rate	0%	0%	0%	0%	0%	62%	69%	69%	65%	70%	70%	70%	82%	82%		
FY26 Total Encumbered and Encumbered	\$ -	\$ -	\$ -	\$ -	\$ 4,800	\$ 1,161,200	\$ 101,800	\$ 4,057	\$ 52,780	\$ 51,150	\$ 142,339	\$ 21,960	\$ 201,544	\$ 1,744,059	\$ 446,134	\$ 755,941
FY26 Burn Rate	0%	0%	0%	0%	0%	47%	51%	51%	53%	55%	61%	63%	70%	70%		
YTD Encumbered & Encumbered	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -
	\$ 2,184,253															

Figure 2: Central Virginia Node FY26 Finance Report

	Budgeted	Jul-25	Aug-25	Sep-25	Oct-25	Nov-25	Dec-25	Jan-26	Feb-26	Mar-26	Apr-26	May-26	Jun-26	Actual YTD	Encumbered Funds	Budget Balance YTD
556002 - CCI - NoVa Node - Operations																
Operations	\$ 300,000	\$ 21,530	\$ 20,596	\$ 21,214	\$ 18,048	\$ 17,917	\$ 16,605	\$ 16,720	\$ 16,725	\$ 16,605	\$ 17,765	\$ 17,660	\$ 19,393	\$ 220,779	\$ -	\$ 79,221
														\$ -		\$ 300,000
														\$ -		
														\$ -		
														\$ -		
														\$ -		
Subtotal	\$ 300,000	\$ 21,530	\$ 20,596	\$ 21,214	\$ 18,048	\$ 17,917	\$ 16,605	\$ 16,720	\$ 16,725	\$ 16,605	\$ 17,765	\$ 17,660	\$ 19,393	\$ 220,779	\$ -	\$ 79,221
Burn Rate		7%	14%	21%	27%	33%	38%	44%	50%	55%	61%	67%	74%	74%		26%
556003 - CCI - NoVa Node - Research																
Faculty Fellows	\$ 200,000	\$ -	\$ 36,485	\$ -	\$ 47,853	\$ -	\$ -	\$ 43,723	\$ -	\$ -	\$ 42,947	\$ -	\$ -	\$ 171,008	\$ -	\$ 28,992
Research Proposals	\$ 400,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 600,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 600,000	\$ -	\$ (200,000)
Undergraduate Research	\$ 90,000	\$ 7,200	\$ 14,840	\$ 6,600	\$ 17,000	\$ 20,800	\$ 18,400	\$ 32,800	\$ 52,000	\$ 35,000	\$ 74,200	\$ 60,289	\$ 14,000	\$ 362,139	\$ -	\$ (282,139)
Research Sprouts	\$ 50,000	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 3,919	\$ -	\$ -	\$ 46,081
RF Shielding Lab	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 200,000	\$ (200,000)
Subtotal	\$ 740,000	\$ 7,200	\$ 51,325	\$ 5,600	\$ 64,853	\$ 20,800	\$ 618,400	\$ 76,523	\$ 52,000	\$ 35,000	\$ 117,147	\$ 64,217	\$ 14,000	\$ 1,127,065	\$ 200,000	\$ (387,065)
Burn Rate		1%	8%	9%	17%	20%	104%	114%	121%	126%	142%	150%	152%	152%		
556005 - CCI - NoVa Node - Workforce Development																
Subsidized Undergraduate Cybersecurity Internships	\$ 277,000	\$ 47,520	\$ 35,920	\$ 14,080	\$ 19,360	\$ 22,880	\$ 56,000	\$ 19,360	\$ 34,320	\$ 22,880	\$ 33,600	\$ 31,880	\$ 27,107	\$ 383,240	\$ -	\$ (85,240)
Traineeships and Apprenticeships	\$ 442,000	\$ 75,600	\$ 104,161	\$ 30,000	\$ 54,000	\$ 24,000	\$ 16,000	\$ 6,000	\$ 34,000	\$ 14,000	\$ 4,000	\$ 12,000	\$ 63,300	\$ 437,261	\$ -	\$ 4,639
Cyber Talent Pipeline Development Program	\$ 145,000	\$ 450	\$ 107,500	\$ 47,552	\$ -	\$ -	\$ 2,500	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 158,002	\$ -	\$ (13,002)
Pilot - Cybersecurity Field Training Experience	\$ 68,000	\$ -	\$ -	\$ -	\$ 6,280	\$ 13,280	\$ 22,800	\$ 19,360	\$ -	\$ -	\$ -	\$ 6,032	\$ 16,420	\$ 84,172	\$ -	\$ (16,172)
Experiential Learning Sprouts	\$ 28,000	\$ 3,117	\$ 6,608	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 5,901	\$ -	\$ -	\$ 1,916	\$ 1,562	\$ 19,105	\$ -	\$ 8,865
														\$ -		\$ 28,000
														\$ -		
														\$ -		
Subtotal	\$ 960,000	\$ 126,687	\$ 254,189	\$ 91,632	\$ 79,640	\$ 60,160	\$ 97,300	\$ 44,720	\$ 74,221	\$ 36,880	\$ 37,600	\$ 51,828	\$ 107,022	\$ 1,081,870	\$ -	\$ (101,870)
Burn Rate		13%	40%	48%	58%	64%	74%	79%	86%	90%	94%	99%	111%	111%		
556006 - NoVa Node - Innovation																
CCI Incubator + Accelerator (CHAP/LT/CCI+)	\$ 500,000	\$ 6,000	\$ 26,559	\$ 2,115	\$ 30,540	\$ 5,557	\$ 3,521	\$ 2,348	\$ 4,462	\$ 4,462	\$ 2,231	\$ 679,577	\$ 2,368	\$ 769,740	\$ 35,162	\$ (304,902)
														\$ -		\$ -
														\$ -		\$ -
														\$ -		\$ -
Subtotal	\$ 500,000	\$ 6,000	\$ 26,559	\$ 2,115	\$ 30,540	\$ 5,557	\$ 3,521	\$ 2,348	\$ 4,462	\$ 4,462	\$ 2,231	\$ 679,577	\$ 2,368	\$ 769,740	\$ 35,162	\$ (304,902)
Burn Rate		1%	5%	7%	13%	14%	15%	15%	16%	17%	18%	19%	19%	154%		161%
FY23 Total Funds Executed	\$ 2,500,000	\$ 161,417	\$ 352,699	\$ 120,591	\$ 193,081	\$ 184,434	\$ 735,827	\$ 140,311	\$ 147,409	\$ 92,947	\$ 174,744	\$ 815,328	\$ 142,763	\$ 3,179,468	\$ 235,162	\$ (714,626)
																\$ 2,500,000

Figure 3: Northern Virginia Node FY26 Finance Report

	Jul-25	Aug-25	Sep-25	Oct-25	Nov-25	Dec-25	Jan-26	Feb-26	Mar-26	Apr-26	May-26	Jun-26	Actual YTD	Budget Balance YTD	Budgeted
556020 - CCI SWVA - Node Research															
Research Projects	\$ 572,397.00						\$ 60,000.00				\$ 179,999.00		\$ 872,396.00	\$ 27,604.00	\$ 900,000.00
Research Personnel	\$ 240,110.00	\$ 128,066.00			\$ 63,430.00			\$ 83,052.00				\$ 15,000.00	\$ 564,558.00	\$ 30,342.00	\$ 595,000.00
Other											\$ 2,082.80	\$ 6,707.09	\$ 5,703.49	\$ 14,493.38	\$ -
Subtotal	\$ 812,507.00	\$ 128,066.00	\$ 128,066.00	\$ -	\$ 60,000.00	\$ 63,430.00	\$ 60,000.00	\$ 83,052.00	\$ -	\$ 35,000.00	\$ 182,081.80	\$ 6,707.09	\$ 1,451,547.38	\$ 43,432.62	\$ 1,495,000.00
Burn Rate	54%	63%	63%	63%	67%	71%	75%	81%	81%	83%	95%	96%	97%	97%	
556021 - CCI SWVA - Node Innovation and Talent Pipeline															
Innovation Projects	\$299,999.00					\$29,975.00	\$100,000.00			\$15,000.00	\$25,000.00		\$469,974.00	-\$147,474.00	\$322,500.00
Workforce Projects	\$119,995.00	\$60,000.00	\$8,000.00			\$305.00	\$126,000.00	\$8,000.00	\$35,000.00	\$31,500.00		\$9,000.00	\$397,711.00	-\$53,711.00	\$344,000.00
Innovation Personnel	\$10,500.00									\$70,500.00			\$81,000.00	-\$70,500.00	\$10,500.00
Outreach costs			\$4,520.00	\$256.94	\$1,068.64	\$1,036.22	\$6,269.09		\$6,500.00	\$6,567.00	\$500.00	-\$5,000.00	\$21,717.89	\$282.11	\$22,000.00
Internal CCI SWVA Interns				\$1,232.70	\$807.52	\$402.64		\$717.30	\$519.00	\$702.45	\$328.50	\$206.64	\$4,916.75	\$1,082.25	\$6,000.00
Other													\$0.00	\$0.00	\$0.00
Subtotal	\$439,494.00	\$60,000.00	\$12,520.00	\$1,489.64	\$1,876.16	\$31,718.86	\$232,269.09	\$8,717.30	\$42,019.00	\$124,289.45	\$25,828.50	\$4,206.64	\$975,316.64	- \$270,316.64	\$705,000.00
Burn Rate	61%	70%	70%	71%	72%	72%	76%	109%	110%	116%	134%	138%	138%		
556022 - CCI SWVA - Node Operations															
Labor	\$60,950.61	\$14,094.76	\$14,676.45	\$13,710.44	\$21,882.06	\$24,143.76	\$12,162.14	\$9,854.80	\$9,854.82	\$9,854.81	\$5,854.80	\$6,431.27	\$207,470.72	\$72,529.28	\$280,000.00
Operating costs			\$106.10	\$2,143.22	\$1,561.60	\$466.78			\$166.14	\$1,773.49	\$549	\$80.74	\$4,536.00	\$5,664.00	\$10,000.00
Travel and Training Costs					\$2,263.03			\$22.71		\$1,773.49	\$12,349.60		\$16,655.71	(\$6,655.71)	\$10,000.00
Subtotal	\$60,950.61	\$14,094.76	\$14,782.55	\$15,853.66	\$25,106.69	\$24,610.54	\$12,162.14	\$9,877.51	\$10,020.96	\$11,877.11	\$22,213.89	\$6,512.01	\$229,062.43	\$70,937.57	\$300,000.00
Burn Rate	20%	25%	25%	30%	35%	44%	52%	56%	59%	63%	67%	74%	76%	76%	
FY26 Total Encumbered	\$ 1,303,951.61	\$ 202,160.76	\$ 27,302.55	\$ 27,302.55	\$ 77,343.30	\$ 116,330.40	\$ 327,483.23	\$ 18,554.81	\$ 87,039.96	\$ 318,228.36	\$ 54,749.48	\$ -31,422.14	\$ 2,655,229.45	\$ (155,229.45)	\$ 2,500,000.00
FY26 Burn Rate	52%	60%	61%	61%	64%	68%	73%	86%	87%	90%	103%	105%	105%	105%	
FY26 Encumbered Funds Executed															
FY25 Research projects				\$5,464.09									\$5,464.09		
FY25 Innovation projects													\$0.00		
FY25 Workforce projects	\$47,000.00			\$75,000.00									\$122,000.00		
FY26 Total Funds Executed	\$ 47,000.00	\$ -	\$ -	\$ -	\$ 80,464.09	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ -	\$ 127,464.09	\$ -	\$ -

Figure 4: Southwest Virginia Node FY26 Finance Report

DESCRIPTION	CODE	1st QTR	2nd QTR	3rd QTR	4th QTR	FY 2026
REVENUE						
Registration Fee	3111	\$330.00	\$325.00	\$4,725.00	\$120.00	\$5,500.00
Receipts Other State Agency	3501	\$654,999.96	\$625,000.00	\$1,024,999.99	\$829,648.23	\$3,134,648.18
Total Revenue		\$655,329.96	\$625,325.00	\$1,029,724.99	\$829,768.23	\$3,140,148.18
EXPENSES						
LABOR						
Administrative Salaries	4001	\$51,110.87	\$27,391.59	\$27,307.88	\$22,965.85	\$128,776.19
Classified Salaries	4002	\$9,508.96	\$0.00	\$8,939.49	\$10,314.80	\$28,763.25
Faculty - Teaching	4005	\$130,969.35	\$186,150.76	\$189,292.30	\$156,725.68	\$663,138.09
IT Salaries	4011	\$28,617.47	\$24,529.26	\$20,441.05	\$20,441.05	\$94,028.83
Grad Asst. Teaching	4022	\$7,000.00	\$0.00	\$0.00		\$7,000.00
Grad Asst Non Teaching	4023	\$1,000.00	\$0.00	\$0.00		\$1,000.00
Student- w/o FICA	4025	\$1,000.00	\$0.00	\$0.00		\$1,000.00
Wages	4031	\$5,875.00	\$7,812.50	\$6,250.00	\$12,912.50	\$32,850.00
Moving & Relocation	4032	\$0.00	\$3,000.00	\$0.00		\$3,000.00
Awards/Honorariums	4034		\$9,586.53	\$0.00	\$10,868.58	\$20,455.11
Bonus	4036	\$0.00	\$0.00	\$0.00	\$15,559.50	\$15,559.50
Mobile Device Allowance	4041	\$315.00	\$270.00	\$270.00	\$225.00	\$1,080.00
Labor Total		\$236,398.66	\$268,740.84	\$262,600.72	\$260,012.98	\$968,860.97
BENEFIT \$						
Employer Retire Cont-VRS Def Ben	4901	\$11,626.34	\$12,468.19	\$12,468.19	\$10,390.15	\$46,952.87
FOAI SALARIED STATE EMP	4902	\$19,689.70	\$13,379.72	\$19,274.12	\$17,990.94	\$70,334.48
Federal Old-Age Insurance for Wage	4903	\$425.86	\$0.00	\$0.00	\$22.95	\$448.81
GROUP LIFE INSURANCE	4904	\$2,054.66	\$2,860.58	\$3,441.15	\$2,483.32	\$10,839.71
HOSPITALIZATION INSURANCE	4905	\$38,135.29	\$29,254.20	\$38,887.20	\$31,218.00	\$137,494.69
Teachers Insurance and Amunity	4906	\$5,747.99	\$3,876.00	\$3,876.00	\$3,217.53	\$16,717.52
VRS HEALTH CARE	4908	\$2,281.68	\$2,714.99	\$3,266.03	\$2,356.96	\$10,619.66
LTD DISABILITY INSURANCE	4920	\$344.61	\$394.92	\$394.92	\$294.01	\$1,428.46
Short Term Disability Benefits	4923	\$0.00	\$9,227.06	\$1,100.25	\$0.00	\$10,327.31
CASH MATCH EXPENSE	4925	\$632.23	\$514.77	\$564.76	\$537.30	\$2,249.06
VA HYBRID RETIREMENT ICMA/RC	4926	\$489.65	\$422.40	\$633.66	\$528.05	\$2,073.76
VRS DCP Optional Retirement	4930	\$8,664.35	\$6,788.93	\$10,366.87	\$8,138.94	\$33,959.09
PRT	4997	\$0.00	-\$107.16			-\$107.16
Benefits Total		\$90,092.38	\$81,784.80	\$94,273.16	\$77,178.16	\$343,338.28
NP \$						
Printing Services	5005	\$0.00	\$110.00	\$0.00	\$1,200.99	\$1,310.99
Telephone Equip	5006	\$322.50	\$322.50	\$322.50	\$380.07	\$1,347.57
Inbound Freight Services	5021	\$230.59	\$0.00	\$0.00	\$178.00	\$408.59
Employee Training/Conferences	5103	\$2,710.00	\$0.00	\$0.00	\$3,560.00	\$6,270.00
Employee IT Training Courses, Workshops	5106	\$0.00	\$0.00	\$60.00	\$390.00	\$450.00
Bank Service Fee	5213	\$8.43	\$17.44	\$101.37	\$50.94	\$178.18
Custodial Services	5301	\$0.00	\$0.00	\$254.56		\$254.56
Plant Repair & Maintenance	5307	\$26.73	\$0.00	\$0.00		\$26.73
Food & Dietary Services	5404	\$1,855.22	\$4,064.35	\$0.00		\$5,919.57
Skilled Services-Indiv	5412	\$0.00	\$0.00	\$841.00	\$6,226.44	\$7,067.44
Computer Software Maint. Svc.	5456	\$23.62	\$0.00	\$0.00		\$23.62
Grants to Non-govt Orgns	5580	\$536,850.90	\$287,404.41	\$99,288.59	\$766,859.49	\$1,690,403.39
Apparel	6001	\$857.93	\$0.00	\$3,643.50	\$695.00	\$5,196.43
Office Supplies	6002	\$2,530.66	\$132.44	\$931.09	\$1,435.89	\$5,030.08
NP \$ Total		\$646,418.68	\$292,051.14	\$106,442.61		
TRAVEL						
Personal Vehicle	7102	\$190.32	\$288.00	\$112.00		\$590.32
Meals	7107	\$0.00	\$0.00	\$0.00	\$2,865.78	\$2,865.78
Employer Travel/Ldngg/Meals	7109	\$147.48	\$2,401.66	\$0.00		\$2,549.14
Travel Pod	7999	\$0.00	\$0.00	\$0.00		\$0.00
Travel Total		\$337.80	\$2,689.66	\$112.00	\$2,865.78	\$6,005.24
Equipment						
Computers <\$5000 ETF	9004	\$559.68	\$0.00	\$0.00		\$559.68
Equipment Total		\$559.68	\$0.00	\$0.00	\$0.00	\$559.68
		1st QTR	2nd QTR	3rd QTR	4th QTR	FY 2026
Revenue Total		\$655,329.96	\$625,325.00	\$1,029,724.99	\$829,768.23	\$3,140,148.18
Expense Total		\$871,803.07	\$836,278.04	\$462,328.48	\$330,068.89	\$2,289,484.48
Labor		\$236,398.66	\$268,740.84	\$262,600.72	\$260,012.98	\$968,860.97
Benefits		\$90,092.38	\$81,794.80	\$94,273.16	\$77,178.16	\$343,338.28
NPS		\$646,418.68	\$292,051.14	\$106,442.61	\$0.00	\$942,910.33
Travel		\$337.80	\$2,689.66	\$112.00	\$2,865.78	\$6,005.24
Equipment		\$559.68	\$0.00	\$0.00	\$0.00	\$559.68
Total (Revenue - Expense)		-\$216,473.11	-\$8,951.04	\$677,396.51	\$499,711.34	\$850,683.70

Figure 5: Coastal Virginia Node FY26 Finance Report

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/>