Fiscal Year 2024 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 2024 REPORT

Commonwealth Cyber Initiative

September 27, 2024

Message from the Executive Director

As we approach our fifth anniversary, the Commonwealth Cyber Initiative (CCI) remains unique in the Nation, with its network of 46 institutions of higher education working together on a common mission of research, innovation, and workforce development in cybersecurity.

The number one factor for technological leadership in this sector is talent development. Every year, CCI creates experiential learning opportunities for hundreds of Virginia students. Through our internship and project-based learning programs, these students work directly with professionals in companies ranging from small startups to the biggest names in tech, as well as in government agencies as varied as the Virginia State Police and the Virginia Department of Elections.

Towards our vision of positioning the commonwealth as a global leader in cybersecurity, this year we held our first international workshop, in collaboration with KU Leuven, one of the leading universities in Europe. One tangible indicator of our leadership in research is the ability of our researchers to successfully compete for federal and private sector funding. We have grown from a baseline of 35M$ in new grants and contracts in Fiscal Year 2020 (FY20) to 112M$ in Fiscal Year 2024 (FY24), a threefold increase in just four years.

In innovation, our two-pronged strategy is to promote the transition of research into commercializable product (through spin-outs, intellectual property licensing, and preparing our researchers for entrepreneurship careers) and to promote the success of Virginia cybersecurity startups (through placements of interns, contributing subject matter expertise, and providing incubator and accelerator services). This year, we also celebrated two more CCI spin-outs incorporated in Virginia!

All of this is the result of the dedication of more than 350 professionals in all corners of the commonwealth who are involved in CCI, as well as thousands of brilliant students. In this annual report, our fifth, you will read about the impact that CCI is achieving in making Virginia a cybersecurity leader.

Luiz DaSilva, Ph.D.; Fellow, IEEE

Executive Director, Commonwealth Cyber Initiative

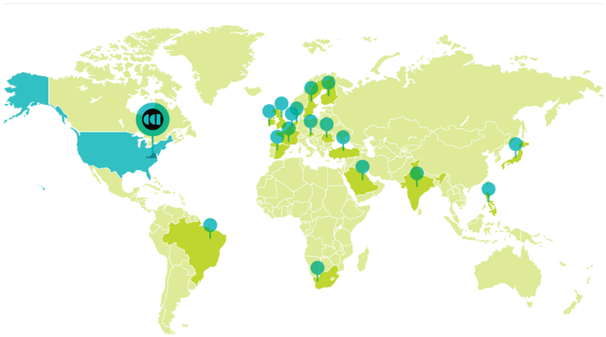
Bradley Professor of Cybersecurity, Virginia Tech

Executive Summary

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

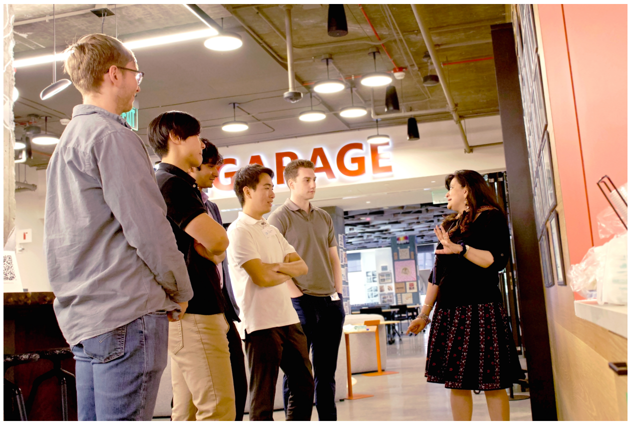
Our ambitious vision is to establish Virginia as a global leader in cybersecurity, and by doing so, help diversify the economy of the commonwealth, attracting private investment and jobs.

In Fiscal Year 2024 (FY24) we continued to see significant increase in new research contracts from sources outside the commonwealth, as well as additional emphasis on our workforce development and innovation programs. Virginia is unique in the country in establishing this large-scale collaboration of institutions of higher education (now with 46), and the investment continues to pay off in jobs (and, crucially, a skilled workforce that can fill those jobs!), spin-outs and startups, and the reputation of our academic institutions. This report highlights some of the major accomplishments in the past fiscal year.

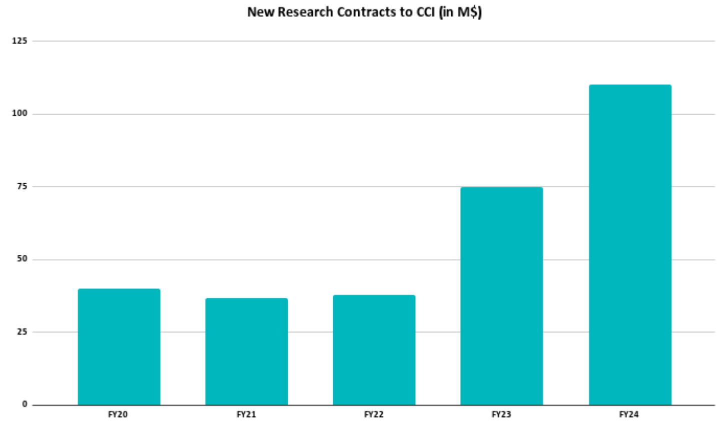


Global Distinction. In line with our goal of establishing Virginia as a global leader in cybersecurity, we have stepped up collaborations with partners in Europe, Asia, and Latin America. In partnership with KU Leuven, one of the leading universities in Europe, we held our first international cybersecurity workshop. Sixty attendees, representing 35 institutions in 10 countries, attended this two-day, invitation-only workshop with the goal of establishing research partnerships in cybersecurity across the Atlantic. Virginia researchers and university leaders collaborated with the European attendees in planning sessions that mapped out key cybersecurity challenges to be addressed with US-Europe partnerships and mechanisms for these collaborations to happen. The workshop resulted in a report being presented to funding agencies on both sides of the Atlantic and other key stakeholders. This year, CCI also joined the International Cybersecurity Center of Excellence (INCS-CoE), an international organization led by universities in the U.S., the U.K., and Japan focusing on international collaborations in cybersecurity research, policy, and education. The CCI Executive Director serves on the board of directors of the organization. Our xG testbed continues to attract international attention, and CCI has hosted delegations from more than 10 countries, often accompanied by representatives from the Department of State and other government agencies.

A Strong Innovation Ecosystem. In the last two years, an estimated 27% of venture capital investments in Virginia were in the field of cybersecurity. CCI continues to contribute to building this ecosystem. In FY24, two new CCI spinouts incorporated in Virginia. These are companies founded by CCI faculty and/or students and that received support from us, usually in early stages of ideation and development of a business plan. The Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) program, co-funded by the CCI Hub and Northern Virginia (NoVA) Node, provides mentorship and financial support for translation of cybersecurity ideas that originate in one of the CCI institutions into commercialization. At the end of each cohort, inventors get to present to a panel of venture capitalists. Pictured here is Dr. Radhika Barua, Assistant Professor at VCU and a researcher funded by CATAPULT, describing to the panel her MagnaShield product, designed to protect hardware from undue electromagnetic interference. The CATAPULT Fund, now in its third year, is critical to advance the maturity of cyber discoveries during the critical ”Valley of Death” phase of commercialization. After the initial funding from this program, innovators are better equipped to progress to SBIR/STTR grants, funding from VIPC, and seed and angel investor funding.



Project-based Learning. There are an estimated 50,000 unfilled cybersecurity jobs in Virginia. Despite this enormous need for new talent, graduating students often find that even entry-level positions require years of experience. Our workforce development programs focus on experiential learning, putting students to work directly with their potential future employers and providing hands-on experience. In our project-based learning program, students work in our industry partners on multi-week cybersecurity projects (while earning an hourly wage). We currently partner with Microsoft and CACI. The cohort shown in the picture included students from Virginia Tech, Christopher Newport University, Laurel Ridge Community College (now attending Old Dominion University), and George Mason University working with Microsoft mentors on a project that investigates cyber vulnerabilities in the use of the Flipper Zero devices. The program is earning rave reviews from students and companies, and we are working on expanding it to more industry partners. Project-based learning is part of a wider portfolio of CCI experimental learning programs that also include internships, traineeships, and others. An annual CCI job and internship fair and Capture the Flag (CTF) events at the regional, commonwealth-wide, and international levels are other important components of our workforce development strategy.



Another Record-breaking Year for Research Funding. The success of the cybersecurity research program in Virginia is evident from scientific breakthroughs being produced by our researchers. It is also measured in research dollars that we are able to bring to fund cybersecurity projects in the commonwealth. We track new research grants and contracts that we obtain every fiscal year, starting at the inception of the initiative. Back in FY20 through Fiscal Year 2022 (FY22), our researchers were bringing approximately $35 million in new research funding per year. Now, in FY24, we brought in $112 million in new grants and contracts, more than triple of our baseline in early days of CCI. This tremendous growth is unheard of and is a testament to the brilliance of the researchers that Virginia is able to attract. It is also a result of CCI's strategy of focusing on team building to go after large-scale research opportunities, as much of the growth can be attributed to increased success in multi-million dollar grants that often require collaboration among researchers in multiple institutions. Approximately 70% of our research funding comes from federal agencies and 30% from the private sector, and the duration of the projects can vary from a few months to five or more years.

Leadership in ORAN. CCI's investments in research infrastructure, in particular the xG testbed, with components at Virginia Tech, Mason, and ODU, has placed us in the leadership of Open Radio Access Network (O-RAN). This year, U.S. Commerce Secretary Gina Raimondo visited CCI to announce a $42 million grant to a project funded by the Wireless Innovation Fund. [She is pictured here at Virginia Tech, with Senator Mark Warner, U.S. Representative Don Beyer, and Assistant Secretary Alan Davidson, National Telecommunications and Information Administration (NTIA) Administrator.] This is one of six projects funded this year by the NTIA with participation from CCI researchers. Open networks are a fundamental component of the U.S. strategy to spur innovation and increase competition in the wireless communications market, and our researchers are worldwide leaders in securing these networks. Forming talent with expertise in O-RAN is a major challenge in the race for leadership in this sector, and CCI is a major contributor to workforce development in this space.

CCI funding is distributed to researchers through open calls for proposals issued both by the Hub and the Nodes. Proposals are peer-reviewed and final recommendations made by CCI's Leadership Council. This ensures that the best ideas, aligned with CCI's mission, are selected for funding in an open and transparent manner.

We continue to be advised by a highly distinguished Technical Advisory Board (TAB), with representatives from industry, state and federal government, academia, and the innovation ecosystem. Some major goals for the coming fiscal year include:

- The launch and execution of CCI 2030, our strategic plan for the next seven years.
- Continued focus on center-scale, multi-million dollar grants involving more than one CCI institution.
- Engagement with industry through a new industry-university cooperation center funded by the National Science Foundation (NSF).
- Capacity building in Virginia on the topic of cybersecurity for Artificial Intelligence (AI) and AI for cybersecurity.
- The launch of a new innovation program and continued support for our incubator and accelerator programs.
- Expansion of international partnerships, strengthening partnerships in Europe and forging new ones in Asia and Latin America.
- Scaling up of our project-based learning program by recruiting additional key industry partners.
- Celebration of our five-year anniversary, communicating CCI's impact to the commonwealth and the Nation.

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project

AI Artificial Intelligence

API Application Programming Interface

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

CBRS Citizens Broadband Radio Service

CCF Commonwealth Commercialization Fund

CCI Commonwealth Cyber Initiative

CoVA Coastal Virginia

CSIIP Commonwealth STEM Industry Internship Program

CTF Capture the Flag

CTO Chief Technology Officer

CVN Central Virginia Node

FY20 Fiscal Year 2020

FY21 Fiscal Year 2021

FY22 Fiscal Year 2022

FY23 Fiscal Year 2023

FY24 Fiscal Year 2024

FY25 Fiscal Year 2025

Mason George Mason University

HR Human Resources

ICAP Innovation Commercialization Assistance Program

IDC Inclusion & Diversity Committee

INCS-CoE International Cybersecurity Center of Excellence

IoT Internet of Things

IUCRC Industry-University Cooperative Research Center

JMU James Madison University

LC Leadership Council

NOFO Notice of Funding Opportunity

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

SDR Software Defined Radio

STEM Science, Technology, Engineering, and Mathematics

SWVA Southwest Virginia

TAB Technical Advisory Board

UVA University of Virginia

VCU Virginia Commonwealth University

VEDP Virginia Economic Development Partnership

VIPA Virginia Innovation Partnership Authority

VIPC Virginia Innovation Partnership Corporation

VMI Virginia Military Institute

VPRI Vice President for Research and Innovation

VSGC Virginia Space Grant Consortium

VT Virginia Tech

VTRC-A Virginia Tech Research Center - Arlington

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

W&M William & Mary

xG Next Generation Networks

Contents

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** at the intersection between **cybersecurity, autonomy, and intelligence**.

This report describes our progress in each of the mission lines in FY24, in pursuit of the vision of global leadership in cybersecurity for the Commonwealth of Virginia.

1.2 The CCI Network

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

1.2.1 An Evolving Network

In FY24, CCI grew again, adding Virginia Wesleyan University in Virginia Beach, VA, to our network. The CCI network now comprises **46** institutions of higher education across Virginia, depicted in Figure 1.1.

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

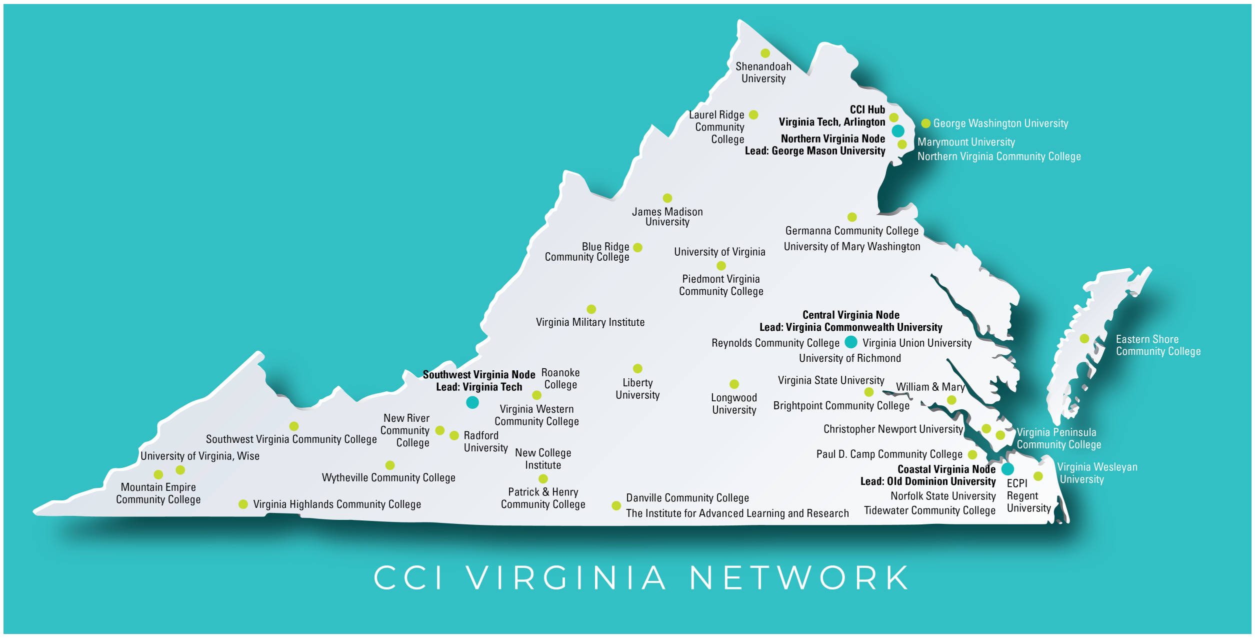

Shenandoah University
Laurel Ridge Community College
CCI Hub
Virginia Tech, Arlington
Northern Virginia Node
Lead: George Mason University
George Washington University
Marymount University
Northern Virginia Community College
James Madison University
Blue Ridge Community College
University of Virginia
Piedmont Virginia Community College
Germanna Community College
University of Mary Washington
Virginia Military Institute
Central Virginia Node
Lead: Virginia Commonwealth University
Reynolds Community College
Virginia Union University
University of Richmond
Eastern Shore Community College
Southwest Virginia Node
Lead: Virginia Tech
Roanoke College
Virginia Western Community College
Liberty University
Longwood University
Virginia State University
William & Mary
Brightpoint Community College
Southwest Virginia Community College
New River Community College
Radford University
Christopher Newport University
Virginia Peninsula Community College
University of Virginia, Wise
New College Institute
Paul D. Camp Community College
Coastal Virginia Node
Lead: Old Dominion University
Virginia Wesleyan University
Mountain Empire Community College
Wytheville Community College
Patrick & Henry Community College
Danville Community College
The Institute for Advanced Learning and Research
ECPI
Norfolk State University
Regent University
Tidewater Community College
Virginia Highlands Community College
CCI VIRGINIA NETWORK

Figure 1.1: The CCI network comprises 46 institutions of higher education across Virginia. Virginia Wesleyan University is the latest member to join.

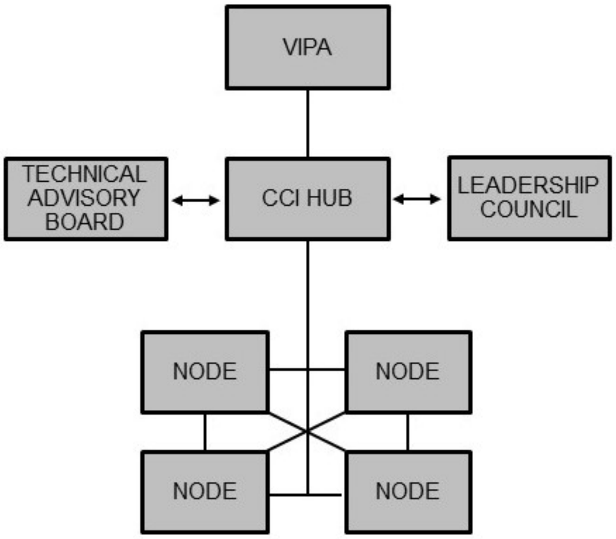
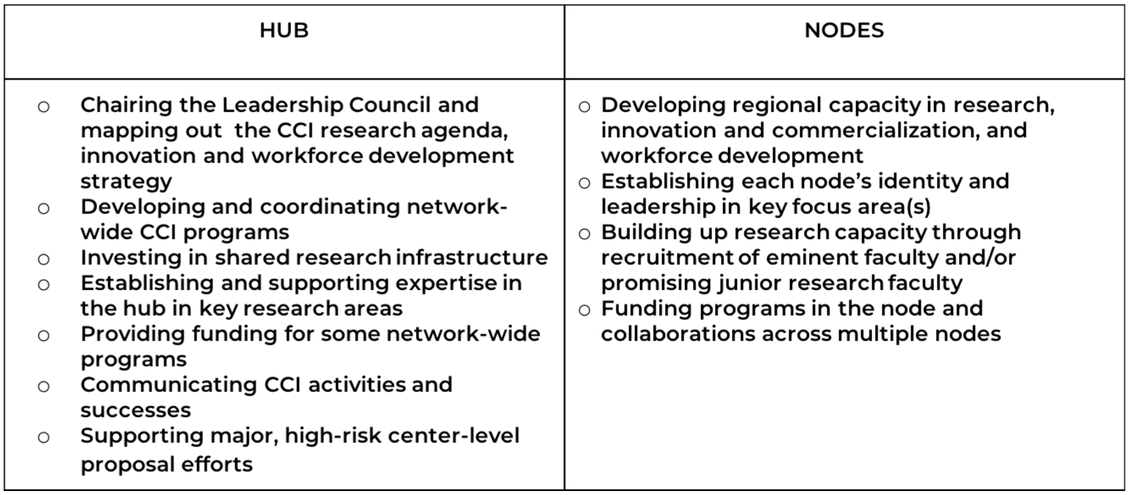


Figure 1.2: CCI governance structure.

The CCI Executive Director chairs the Leadership Council (LC) and is responsible for articulating the research agenda and the innovation and workforce development strategy for the network. The CCI Hub designs, coordinates, and funds network-wide programs and deploys key research infrastructure available to all CCI researchers. The Hub also houses faculty and graduate students with established expertise in key research areas in cybersecurity, autonomous systems, and intelligence. A communications team in the Hub is responsible for external dissemination of CCI activities and successes. Finally, the Hub convenes teams throughout the network to put together large, multi-million dollar research proposals for external funding. The CCI regional Nodes are responsible for developing capacity in research, innovation, and workforce development in their respective geographic regions, establishing leadership in key focus areas. They also recruit eminent faculty and promising junior faculty for their member institutions and fund programs in the Node, as well as collaborations across multiple Nodes. The main roles of the Hub and the Nodes are summarized in Figure 1.3.



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

Figure 1.3: Roles of the CCI Hub and Nodes.

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

Dr. Brian Payne, who served as the CoVA Node Director from the inception of CCI until 2024, has stepped down from that role to become Interim Provost at ODU. CCI is indebted to Dr. Payne for his numerous contributions to the initiative.

1.2.2 CCI Hub Organization and Research Infrastructure Development

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

The CCI Hub occupies dedicated space in Virginia Tech's Arlington Research Center for CCI personnel, laboratories, and an Next Generation Networks (xG) testbed, depicted in Figure 1.6. This is the largest testbed of its kind, with the latest generation of software-defined radios and an end-to-end open implementation of 5G, with capabilities to test new technologies expected beyond 5G. It accessible by CCI researchers

(a) Dr. Luiz DaSilva, Executive Director.

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

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

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

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

(f) Mr. John Delaney, Managing Director.

Figure 1.4: CCI Leadership Council.

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.

An outdoor component of the xG testbed is currently being deployed in the Blacksburg campus of VT. This outdoor testbed will offer unique opportunities for testing and validation of new wireless network technologies being developed for 6G and will use VT's Citizens Broadband Radio Service (CBRS) spectrum licenses. Three site locations have been selected around Stroubles Creek in Blacksburg, VA; these are shown in Figure 1.7. The first of these three site locations has been set up this year and is located on the HABBI building rooftop. The cabinet installed at that site is shown in Figure 1.8. This site has a CBRS base station connected to a 5G core deployed in the edge server and an OpenSAS deployed in the Virginia Tech Research Center - Arlington (VTRC-A) cloud. Two new Dell Power Edge Servers have been purchased for sites 2 and 3 of the outdoor testbed.

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 count with a lean communications and marketing team.

The CCI CoVA Node is headquartered in ODU's facilities in Virginia Beach, VA. The Node dedicated $17,000 in FY24 to infrastructure upgrades/life cycle for the COVA SHARE servers. Two new Nutanix NX-3155G-G8 nodes were funded to expand the capabilities of the CCI academic environment. These Nutanix nodes have 1 TB RAM per node, 2x Intel Xeon Gold, 3 GHz, 22TB of storage per node, and Nvidia L40's GPU specifications. The lab space dedicated to CCI student researchers is depicted in Figure 1.9.

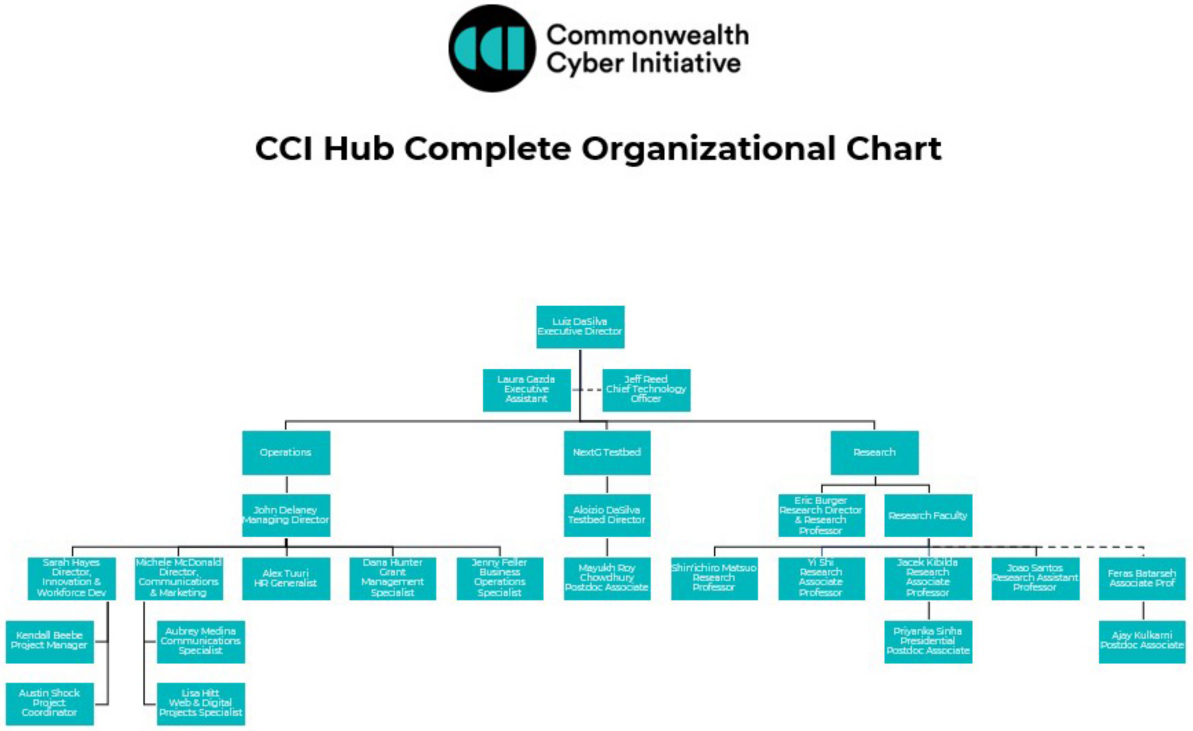

Commonwealth Cyber Initiative
CCI Hub Complete Organizational Chart
Luiz DaSilva Executive Director
Laura Gazda Executive Assistant
Jeff Reed Chief Technology Officer
Operations
NextG Testbed
Research
John Delaney Managing Director
Aloizio DaSilva Testbed Director
Eric Burger Research Director & Research Professor
Research Faculty
Sarah Hayes Director, Innovation & Workforce Dev
Michele McDonald Director, Communications & Marketing
Alex Tuuri HR Generalist
Dana Hunter Grant Management Specialist
Jenny Feller Business Operations Specialist
Mayukh Roy Chowdhury Postdoc Associate
Shin'ichiro Matsuo Research Professor
Yi Shi Research Associate Professor
Jacek Kibilda Research Associate Professor
Joao Santos Research Assistant Professor
Feras Batarseh Associate Prof
Kendall Beebe Project Manager
Austin Shock Project Coordinator
Aubrey Medina Communications Specialist
Lisa Hitt Web & Digital Projects Specialist
Priyanka Sinha Presidential Postdoc Associate
Ajay Kulkarni Postdoc Associate

Figure 1.5: CCI organization chart.

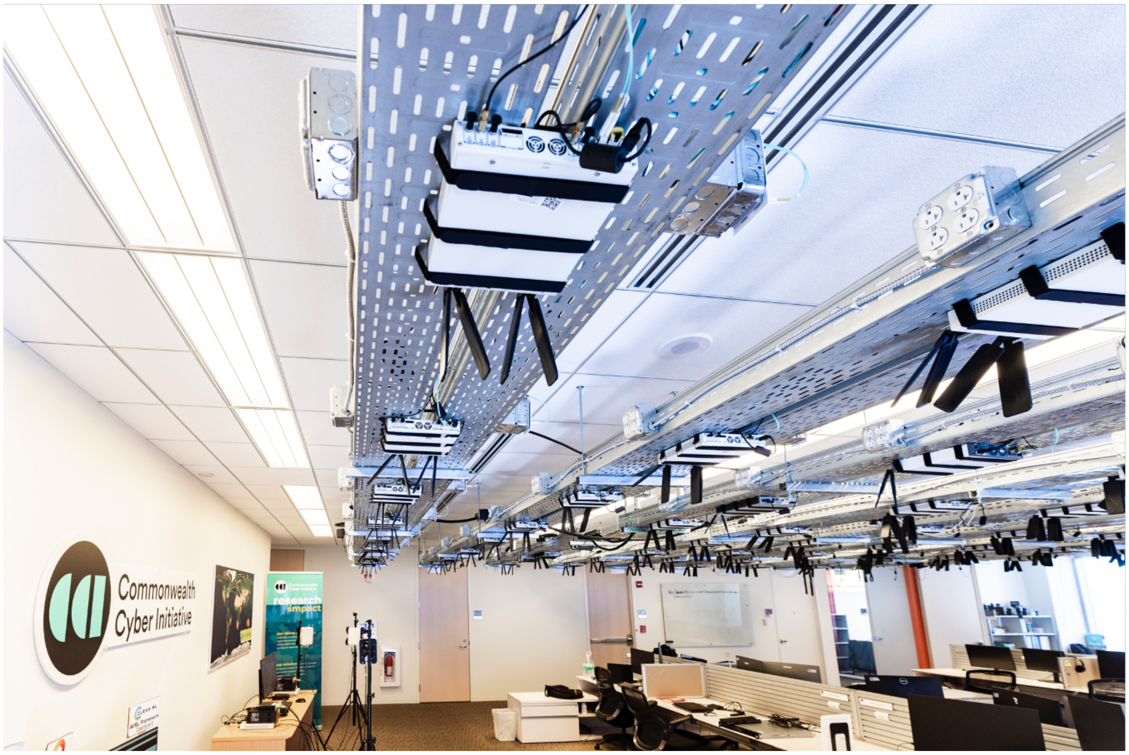


Figure 1.6: CCI xG testbed, indoors portion, in CCI Hub at Virginia Tech.

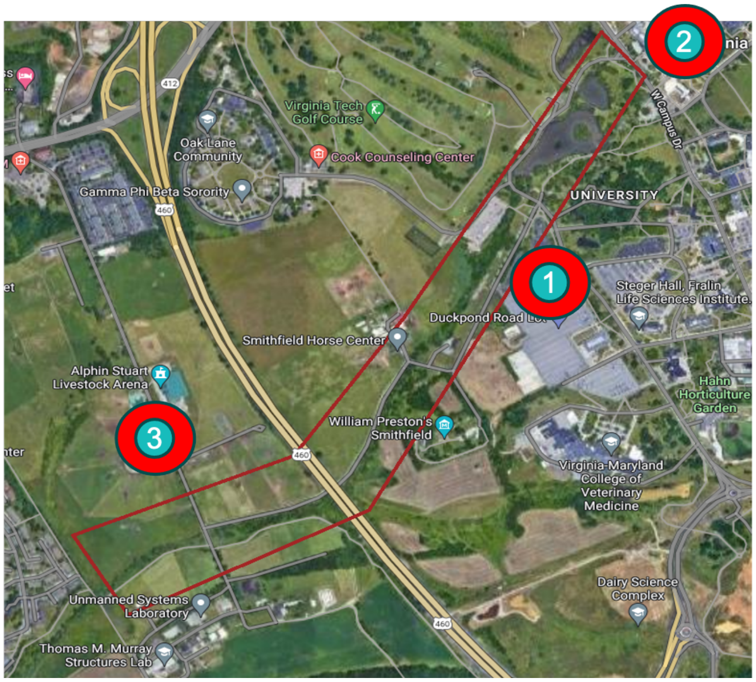

2
nia
412
Virginia Tech Golf Course
W Campus Dr
Oak Lane Community
Cook Counseling Center
Gamma Phi Beta Sorority
460
UNIVERSITY
1
Steger Hall, Fralin Life Sciences Institute
Duckpond Road Lot
Smithfield Horse Center
Alphin Stuart Livestock Arena
Hahn Horticulture Garden
3
William Preston's Smithfield
Virginia-Maryland College of Veterinary Medicine
Unmanned Systems Laboratory
Dairy Science Complex
Thomas M. Murray Structures Lab

Figure 1.7: Sites of the outdoor component of the xG testbed in Blacksburg, VA.

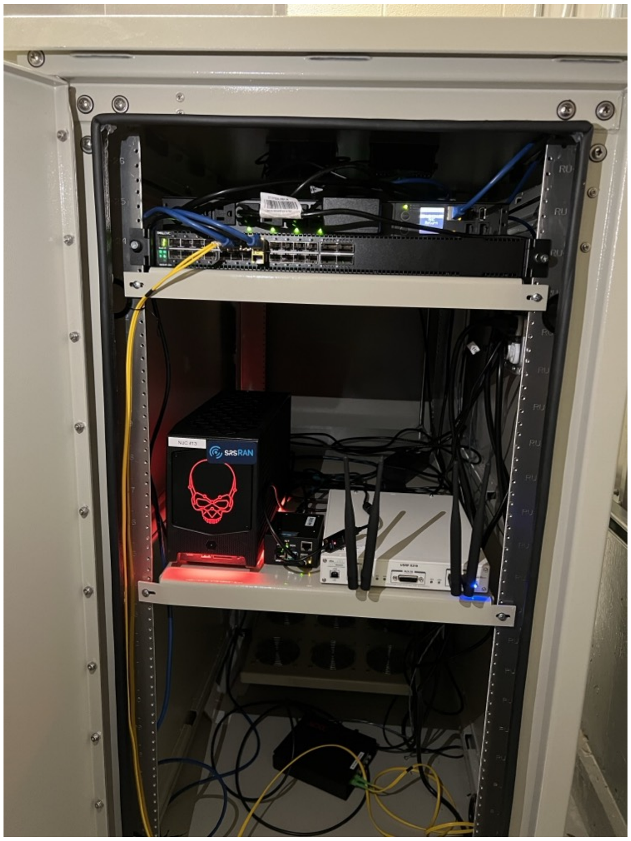


Figure 1.8: The cabinet installed for the outdoor CBRS-based xG testbed.

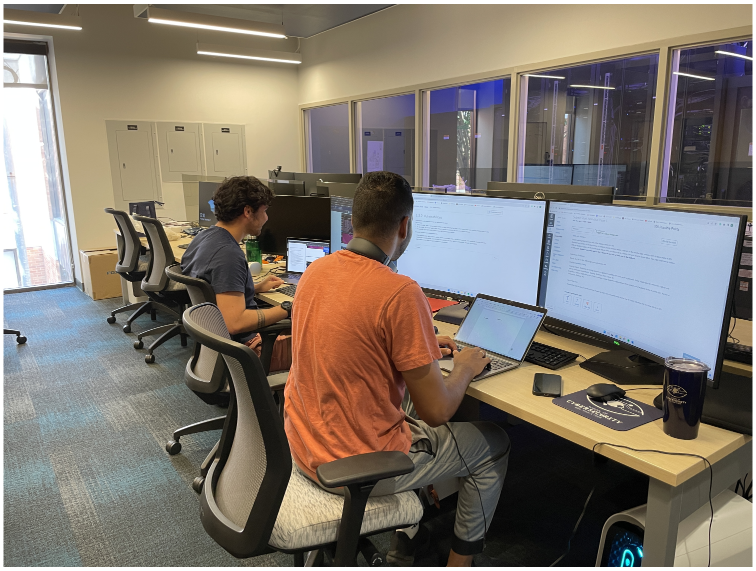


Figure 1.9: COVA CCI Lab Space.

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; and
- One representative from government.

We are fortunate to have an extremely distinguished TAB. Its members are (Figure 1.10):

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

(a) Prof. Elisa Bertino. (b) Mr. David Ihrie. (c) Dr. Anthony Tongen. (d) Prof. Sennur Ulukus.

(e) Ms. Tracy Gregorio. (f) Mr. Jim Mollenkopf. (g) Mr. Zachary Tudor. (h) Mr. Dan Woolley.

Figure 1.10: CCI Technical Advisory Board (TAB).

The full TAB meets twice a year. FY24's Fall meeting, on August 31, 2023, was held in person at the VT-ARC, in Arlington, Virginia, with TAB members and the CCI Leadership Council in attendance. The agenda included: a briefing on the State of CCI by the Executive Director, Luiz DaSilva; a presentation on CCI's Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT) funded innovation work by Radhika Barua from VCU; a presentation by Jack Davidson about the Cyber Navigator program led by University of Virginia (UVA) and involving six CCI universities; a research presentation on cyber biosecurity by Feras Batarseh, VT; an update by Gisele Stolz, George Mason University (Mason), on the CCI Experiential Learning Internship Program; as well as an xG Testbed demonstration and tour by CCI Testbed Director Aloizio Pereira da Silva. The 2030 Strategic Plan was presented by the CCI Director of Workforce Development and Innovation, Sarah Hayes, and the TAB reviewed, provided input and discussed the plan. Time was also set aside for open discussion and advice from the TAB.

FY24's Spring meeting, held on February 29, 2024, was held virtually with TAB members and the CCI Leadership Council in attendance. The agenda included: a briefing on the State of CCI by the Executive Director, Luiz DaSilva; an update on workforce development and innovation by CCI Director of Workforce Development and Innovation, Sarah Hayes; a TAB charter discussion and a CCI Symposium update by CCI Managing Director, John Delaney; and research project updates by Duminda Wijesekera Mason and Aloizio Pereira da Silva, CCI xG Testbed Director. 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 2024. The award recognizes an individual, team, group, or organization who, 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 Dr. Sachin Shetty, a professor at ODU (Figure 1.11).

Dr. Sachin Shetty is the Executive Director of the Center for Secure and Intelligent Critical Systems. The Center researches cyber resilience, data provenance, adaptive models for detecting threats, and practical issues in cloud computing/cyber-physical systems, mobile security, anomaly detection, moving target defense, and risk management. The center participates in several federally-funded centers of excellence, has sixteen personnel supporting research, and regularly contributes to the open-source community. Dr. Shetty's leadership has impacted coastal Virginia by leading offshore wind security and safe and secure port operations. He has contributed to the standards community as subgroup chair on the Internet of Medical Things, IEEE P2418.6 Standards Development Working Group. His cybersecurity research impact extends internationally, as a Fulbright Specialist at the University of Iceland and through the development of learning modules for graduate students in Greece and Iceland. He has authored or co-authored over 200 research

Figure 1.11: Dr. Sachin Schetty, ODU, FY24's CCI Impact Award winner.

articles in journals and conference proceedings and edited four books. He is the recipient of the Fulbright Specialist award, the top 2 percent cited scientist in the world, the top 50 Influential papers in Blockchain award, the EPRI Cybersecurity Research Challenge award, the Commonwealth Cyber Initiative Fellowship award, three-time DHS Scientific Leadership award and has been inducted in Tennessee State University's million dollar club.

1.4 The CCI Inclusion and Diversity Committee

To increase the participation of under-represented groups in the cyber workforce is one of the strategic goals of CCI:

Strategic Goal

CCI will contribute to increasing the diversity of the cybersecurity workforce, so that the composition of that workforce approximates the gender, racial, and ethnicity distribution of the nation's population. It will also foster a culture of inclusion in the work environment, where everyone is treated fairly and respectfully, regardless of age, gender, ethnicity, religion, disability, or sexual orientation.

To fulfill this strategic goal, CCI has established an Inclusion & Diversity Committee (IDC) with the role of advising the LC on matters of inclusion and diversity. The committee itself has diverse representation from CCI-affiliated institutions throughout the commonwealth. The role of the committee is to advise CCI's LC on matters of inclusion and diversity, including:

- The establishment of programs that aim at increasing participation of underrepresented groups in the cyber workforce;
- Diversity goals and considerations in all programs funded by CCI;
- Organization of seminars, workshops, and training events that highlight diversity issues of particular relevance to CCI research, such as gender and racial bias in AI systems, and consideration of persons with disabilities in the design of autonomous systems;
- Outreach activities geared towards underrepresented groups in Science, Technology, Engineering, and Mathematics (STEM).

The IDC is chaired by Dr. Nathan Carter, chief diversity, equity, and inclusion officer at Northern Virginia Community College (NVCC). During the fiscal year, the committee expanded its roster to include two industry representatives and increased its impact. Additional members are:

- Patty Bernardo, CACI International;
- Jacek Kibilda, CCI;
- Jordan Mason, Mason;
- Michele McDonald, CCI;
- Betty Myrthil, Cisco Systems;
- Krzysztof Rechowicz, ODU;
- Joao Santos, CCI;
- Arianna Schuler Scott, VT;
- Yanxiao Zhao (replacing Jennifer Allen), VCU.

In FY24, the CCI Inclusion and Diversity Committee helped develop CCI's new research program, Addressing Inclusion and Accessibility Issues in Cybersecurity (Inclusive Cybersecurity). The program attracted 33 proposals, far exceeding expectations. CCI awarded 11 projects to researchers from Mason, ODU, UVA, VT , and William & Mary (W&M). Projects include such topics as secure authentication for people with disabilities, inclusive biometric authentication, brain-computer interface for password input, judgments by artificial intelligence tools, and more. This program is further discussed in Section 2.2.2.

The committee is organizing a workshop to be held in Fiscal Year 2025 (FY25), in which Virginia researchers will discuss collaborations in inclusive cybersecurity to pursue external funding for large projects and possibly, research centers. In addition, CCI is encouraging researchers to publish papers and lead a research publication dedicated to the topic of inclusive cybersecurity. We are excited about the opportunities for Inclusive Cybersecurity and how it could expand Virginia's reputation as a global leader in the field.

In this fiscal year, the IDC also provided invaluable advice and input to CCI 2030, our strategic plan for the next six years.

1.5 CCI Communications

1.5.1 CCI Social Media Strategy, Website, and Metrics

The CCI Communications and Marketing team continues to grow CCI's reputation and outreach through our website, social media accounts, videos, brochures, one-pagers, monthly newsletter, email campaigns, news stories, external media relations, events, the annual CCI Symposium, and more. Our visual identity has matured, creating a cohesive look across our platforms and programs.

The communications team supports CCI's mission lines of innovation, workforce development, and research, collaborating with leadership to ensure messaging and materials are consistent and on point. The communications team also has expanded its mission to include leading the Research Showcase, CyberArts Program, and Addressing Inclusion and Accessibility in Cybersecurity Research Program.

In this fiscal year, we led the organization of the CCI CyberArts Exhibit, which officially opens with a reception on Oct. 18, 2024 and will be open to the public from October 2024 to mid-January 2025 at the Torpedo Factory Art Center in Alexandria, VA. About 15,000 people are expected to visit the cybersecurity-themed exhibit.

We have enhanced CCI's robust website with expanded funded projects webpages, a 200-plus strong researcher directory, an xG Testbed website, additional workforce development programs, calls for proposals, and other resources. All are designed to be easy to navigate.

Our outreach and increased content have translated to a record 47,672 users in FY24, a 30.5% rise from the prior year (Figure 1.12). CCI website users clicked 379,944 times.

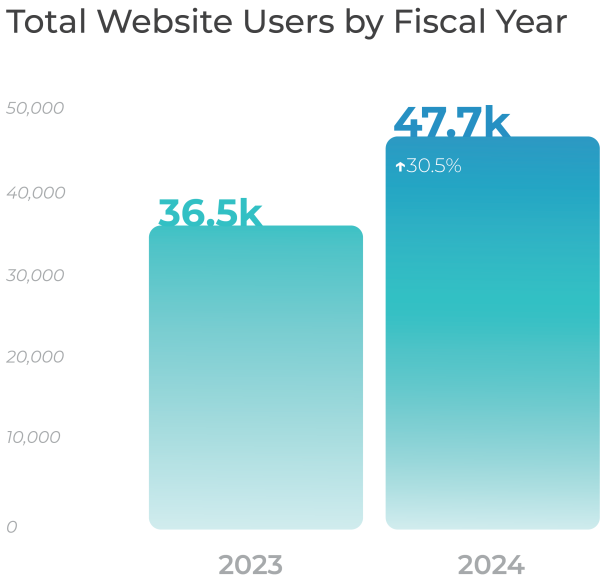


Figure 1.12: Website usage, focusing on users, comparing FY24 to FY23.

Our monthly newsletter keeps our highly engaged audience informed while guiding them to the website. Newsletter subscribers increased to 4,052, from 300 in October 2020.

Our social media accounts, designed to drive people to the CCI website to learn more about our programs and mission, continue to be one of our strongest outreach strategies. Consistent, informative, and engaging posts have led to more people following these posts.

The main CCI LinkedIn account remains our powerhouse and the place where industry partners, researchers, and students share information and successes. Highlights include:

- Our LinkedIn audience grew to 2,741 followers, a 50.1% increase from FY23.
- Our Instagram account now has 283 followers, a 73.5% increase.
- Our Twitter account grew to 605 followers, a 30.4% increase.

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

1.5.2 Appearances in the Media in FY24

Many of the programs and major achievements from CCI researchers and staff have appeared in the print and online media. We posted 252 news stories from or about universities and colleges in the CCI network during the fiscal year. Please visit the news section of our website for more news.

A sampling of media appearances is provided below:

Richmond Times-Dispatch Op-Ed by Luiz DaSilva: To protect the nation, Virginia must remain an innovation leader

CCI fosters international collaboration to counter global cybersecurity threats

CCI named one of 15 specialized wireless testing centers in the world

CCI and CHIPS and Science Act of 2022, Public Wireless Supply Chain Innovation Fund

Federal funding boosts CCI wireless network security projects

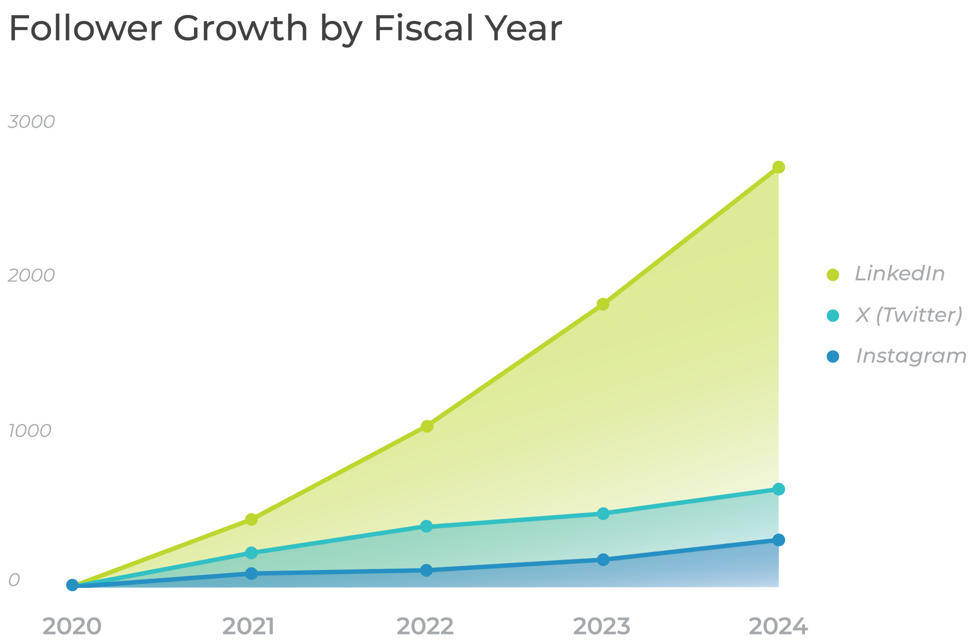


Figure 1.13: Social media followers for CCI's LinkedIn, Instagram, and Twitter accounts.

CCI researchers to hold prominent role in 42 million dollar wireless project

Mason faculty part of NTIA Wireless Innovation Fund project using AI to test O-RAN components

Innovation Fund projects to Virginia Tech promise to unlock potential, secure the future of open networks

CCI named one of 15 specialized wireless testing centers in the world

'Curious Conversations' podcast with Luiz DaSilva about the future of wireless networks and CCI's testbeds

Impact of CCI on the commonwealth

Northern Virginia Magazine: CCI Partners UVA and Virginia Tech: How the Rivals are Stronger Together

Cyber interns compete to capture the flag

15 students join CCI cyber pre-apprenticeship program

CCI funds 11 'inclusive cybersecurity' projects from across Virginia

Virginia Tech researchers work to secure power grid communication on military bases

CCI funds 11 'inclusive cybersecurity' projects from across Virginia

NSA, Homeland Security Name Mountain Empire Community College a National Center of Excellence in Cyber Defense

American Scientist article with CCI Southwest Node Director Gretchen Matthews: The future of cybersecurity hinges on creating harder problems

First Short-term Cyber Security Training Cohort Kicks Off at Danville Community College

Mason University redesignated as a National Center of Academic Excellence

Student teams tackle tech industry challenges at CCI-sponsored PatriotHacks 2023

Water Environment and Technology Magazine: 'Cyber-physical' approach at Virginia Tech's ACWA Lab protects water systems from hackers

Radford University's Classroom to Career Cybersecurity Summit highlights cybersecurity careers for rural students

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

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

CCI researchers recognized

CCI Northern Node Director Liza Wilson Durant among Northern Virginia Technology Council's 2023 Cyber50 Honorees

CCI Research Director Eric Burger elected fellow of National Academy of Inventors

CCI Research Director Eric Burger elected AAAS Fellow

FBI presents VCU's Milos Manic with leadership award for work advocating cybersecurity and outreach programs

UVA Engineering's Jack Stankovic Receives Prestigious IEEE Medal

Largest Computing Society Says UVA's Aidong Zhang and Jack Davidson Among 7 Best

Virginia Tech professor Walid Saad among most highly cited researchers in the world

Highly cited researchers 2023: Wenjing Lou

1.6 Report Structure

This report describes the CCI's progress and achievements in FY24. Chapter 1 outlines our vision and mission, describes the organization of the CCI Hub and Nodes, and summarizes our media strategy. Progress on the three mission lines of research, workforce development, and innovation is described in Chapters 2, 3, and 4, respectively. Chapter 5.1 is devoted to CCI's collaborative partnerships and projects. Chapter 6 contains the financial reports from the hub and nodes for FY24. Finally, Chapter 7 describes our main activities and programs planned for FY25.

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 FY24 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 FY24

In FY24, the CCI network received 138 external grants totaling $112,152,250 to support the CCI mission lines of research, workforce development and innovation. 95 grants (69%) were from federal agencies and 43 (31%) were from state and industry partners. Summary information is shown in Figure 2.1 and details are found in Appendix 1.

2.2 Research Grants Awarded from the Funds in HB30

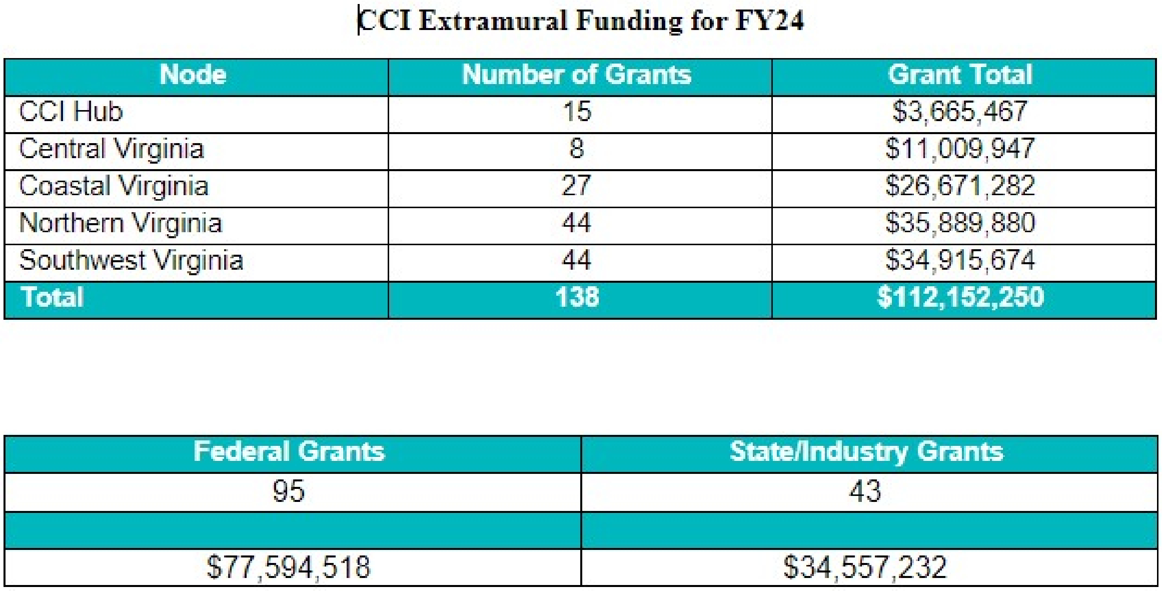
In FY24, CCI awarded grants to the participating institutions, aligned with our goals in research, workforce development, and innovation. These funds were awarded on a competitive basis, with researchers responding to calls for proposals issued by CCI. Proposals were reviewed by experts in the area of each call, and the LC made final funding decisions based on recommendations from reviewers. This section describes the grants awarded in this Fiscal Year from CCI funds.

2.2.1 Research in Supply Chain Cybersecurity

Objective of the Call

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

- Zero-trust architectures;
- Securing softwarized and disaggregated networks;
- Testing and validation of system security;



CCI Extramural Funding for FY24

Node	Number of Grants	Grant Total
CCI Hub	15	$3,665,467
Central Virginia	8	$11,009,947
Coastal Virginia	27	$26,671,282
Northern Virginia	44	$35,889,880
Southwest Virginia	44	$34,915,674
Total	**138**	**$112,152,250**

Federal Grants	State/Industry Grants
95	43
$77,594,518	$34,557,232

Figure 2.1: External funding obtained by the CCI network in FY24.

- Cybersecurity risks to the semiconductor supply chain, including hardware Trojans;
- Autonomous vehicle supply chain security;
- Supply chain security over the product lifetime, e.g., software updates;
- Supply chain security for systems involving artificial intelligence/machine learning.

Objectives of this call include:

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

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

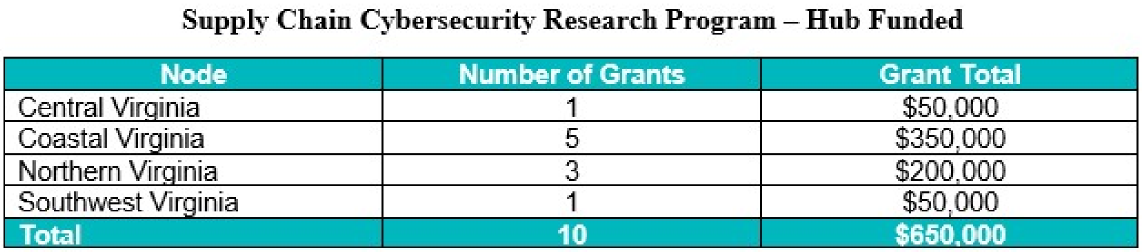
Selection Criteria

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

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

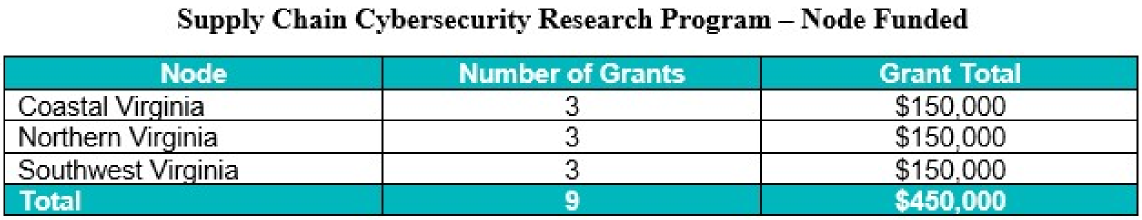
Research Grants Awarded

The CCI Hub awarded and funded 10 grants. The Northern Virginia Node, Coastal Virginia Node, and Southwest Virginia Node each funded an additional 3 grants. The number and value of grants associated with each CCI Node are tabulated in Figure 2.2. Individual grants are listed in the Appendix 2.



Supply Chain Cybersecurity Research Program – Hub Funded

Node	Number of Grants	Grant Total
Central Virginia	1	$50,000
Coastal Virginia	5	$350,000
Northern Virginia	3	$200,000
Southwest Virginia	1	$50,000
Total	**10**	**$650,000**



Supply Chain Cybersecurity Research Program – Node Funded

Node	Number of Grants	Grant Total
Coastal Virginia	3	$150,000
Northern Virginia	3	$150,000
Southwest Virginia	3	$150,000
Total	**9**	**$450,000**

Figure 2.2: Supply Chain Cybersecurity Research Program details for FY24.

2.2.2 Addressing Inclusion and Accessibility in Cybersecurity Program

CCI is dedicated to improving and addressing inclusion, accessibility, and diversity in cybersecurity on a variety of fronts, from the composition of the cybersecurity workforce to the design of technology and systems that affect daily life.

With this program, CCI is building research capacity in the new area of *inclusive cybersecurity*, involving a transdisciplinary response that includes physical, cognitive, financial, and emotional vulnerabilities. Examples include, but are not limited to:

- Accessible and secure digital protection;
- Skin tone or gender bias in artificial intelligence used in cybersecurity;
- Online deception of vulnerable populations;
- Secure systems that can be used by people with disabilities and social and/or economic challenges.

Objective of the Call

Objectives of this program include:

- To produce seminal contributions to address inclusion, accessibility, and diversity issues that are specifically related to cybersecurity;
- To use the program's seed funding to pursue continuation of the awarded project's impact, including but not limited to seeking additional funding from federal and state agencies, foundations, and the private sector;
- To contribute to workforce development in cybersecurity with cross-disciplinary domain knowledge;
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) at the intersection of cybersecurity and accessibility and inclusion.

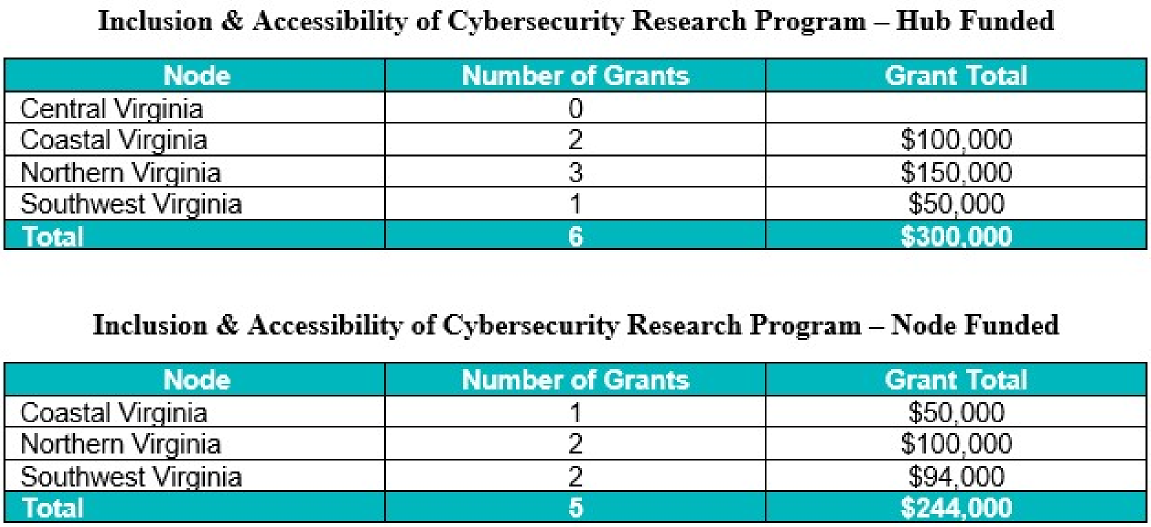
Selection Criteria

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

- Strong intellectual merit related to cybersecurity that addresses inclusion, accessibility, and diversity;
- Relevance to the focus of the call (intersection between cybersecurity and inclusion, accessibility, and diversity);
- Tangible outcomes and likelihood of additional impact in innovation, research, and/or workforce development, through follow-up activities listed in the proposal. Proposers were asked top cite specific programs that could fund and expand the work, including funding agencies, partnerships with philanthropic organizations, foundations, intellectual property, and entrepreneurship opportunities.

Research Grants Awarded

The CCI Hub awarded and funded 6 grants. The Northern Virginia Node awarded 2 grants, the Coastal Virginia Node awarded 1 grant, and the Southwest Virginia Node awarded 2 grants. The number and value of grants associated with each CCI node are tabulated in Figure 2.2. Individual grants are listed in Appendix 2.



Inclusion & Accessibility of Cybersecurity Research Program – Hub Funded

Node	Number of Grants	Grant Total
Central Virginia	0	
Coastal Virginia	2	$100,000
Northern Virginia	3	$150,000
Southwest Virginia	1	$50,000
Total	6	$300,000

Inclusion & Accessibility of Cybersecurity Research Program – Node Funded

Node	Number of Grants	Grant Total
Coastal Virginia	1	$50,000
Northern Virginia	2	$100,000
Southwest Virginia	2	$94,000
Total	5	$244,000

Figure 2.3: Addressing Inclusion and Accessibility in Cybersecurity Research Program details for FY24.

2.2.3 Node Funded Research Projects 2024

In FY24, the CCI Regional Nodes awarded and funded 40 research programs totaling $2,539,858 in research grants. The research projects are focused on a wide-range of cybersecurity topics, such as supply chain security, artificial intelligence, smart technologies, Internet of Things, autonomous systems, wireless network security and 6G. Additionally, numerous projects are multi-disciplinary and are collaborative efforts with research teams from several universities in Virginia. A detailed list of the Node research projects are listed in the figures below:

- Central Node - Figure 2.5
- Coastal and Northern Nodes - Figure 2.6
- Southwest Node - Figures 2.7 and 2.8

The total value of research grants provided by each CCI Node to researchers in their region is shown in Figure 2.4.

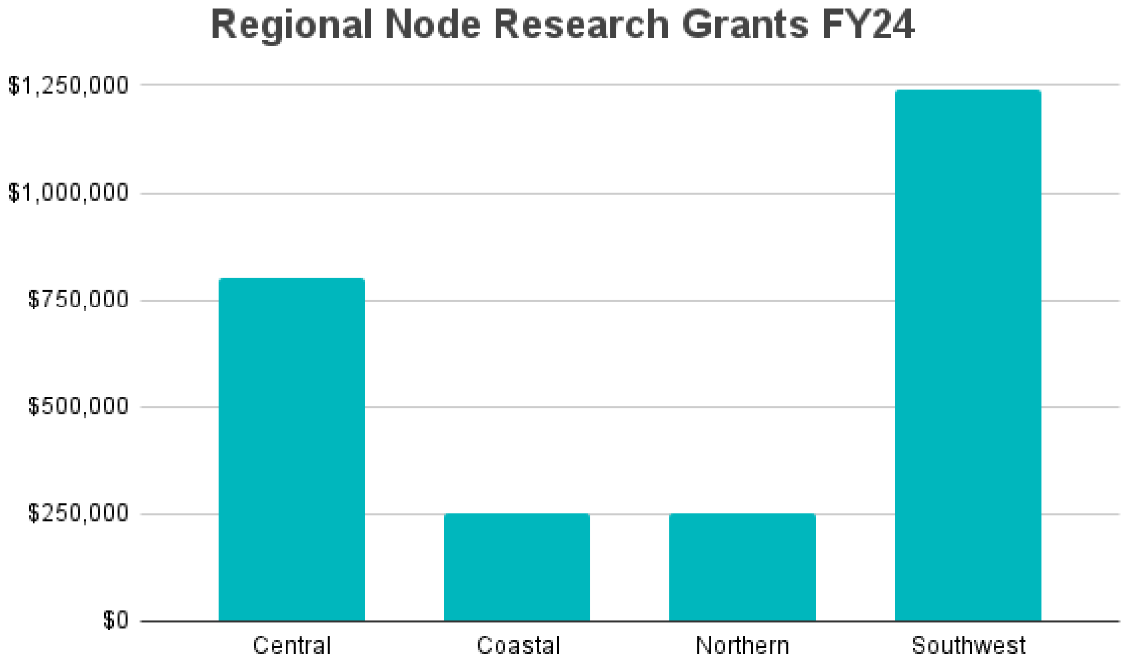


Figure 2.4: Regional Node Research Grants Awarded for FY24.

2.2.4 CCI Fellows Program 2024

This program, launched in FY22 and continued throughout Fiscal Year 2023 (FY23) and FY24, has the objective of supporting large-scale proposals for extramural funding involving three 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

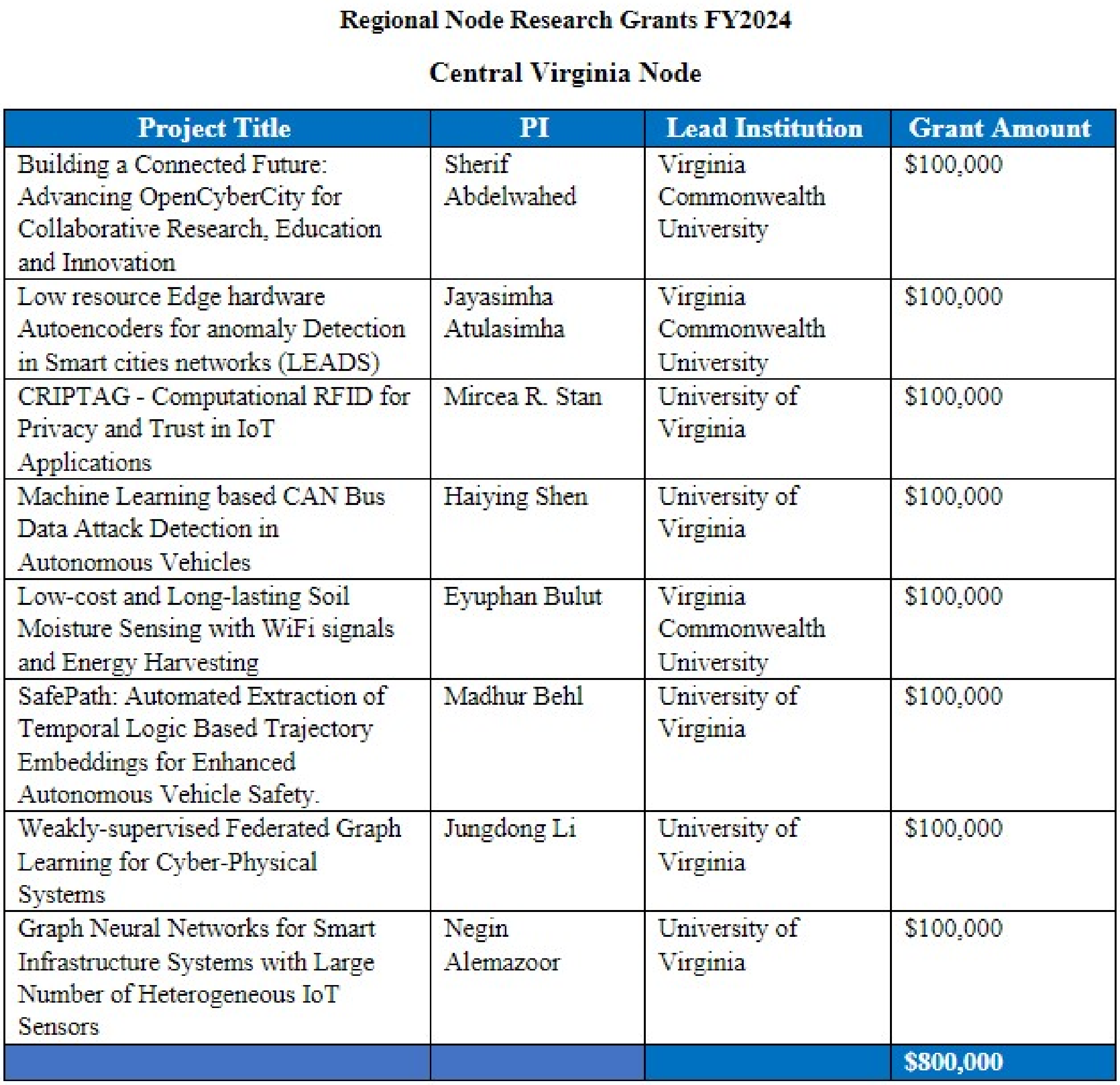
This call funds CCI researchers to lead center-scale proposals. PIs funded under this call are designated as CCI Fellows. Proposals must involve at least two CCI institutions of higher education (from any Node). A CCI institution of higher education must play a coordination role in the project. The budget 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 FY23.

Selection Criteria

Proposals are evaluated 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 FY24 CCI Fellows are listed in Figure 2.9; they join six Fellows funded in FY23.



Regional Node Research Grants FY2024

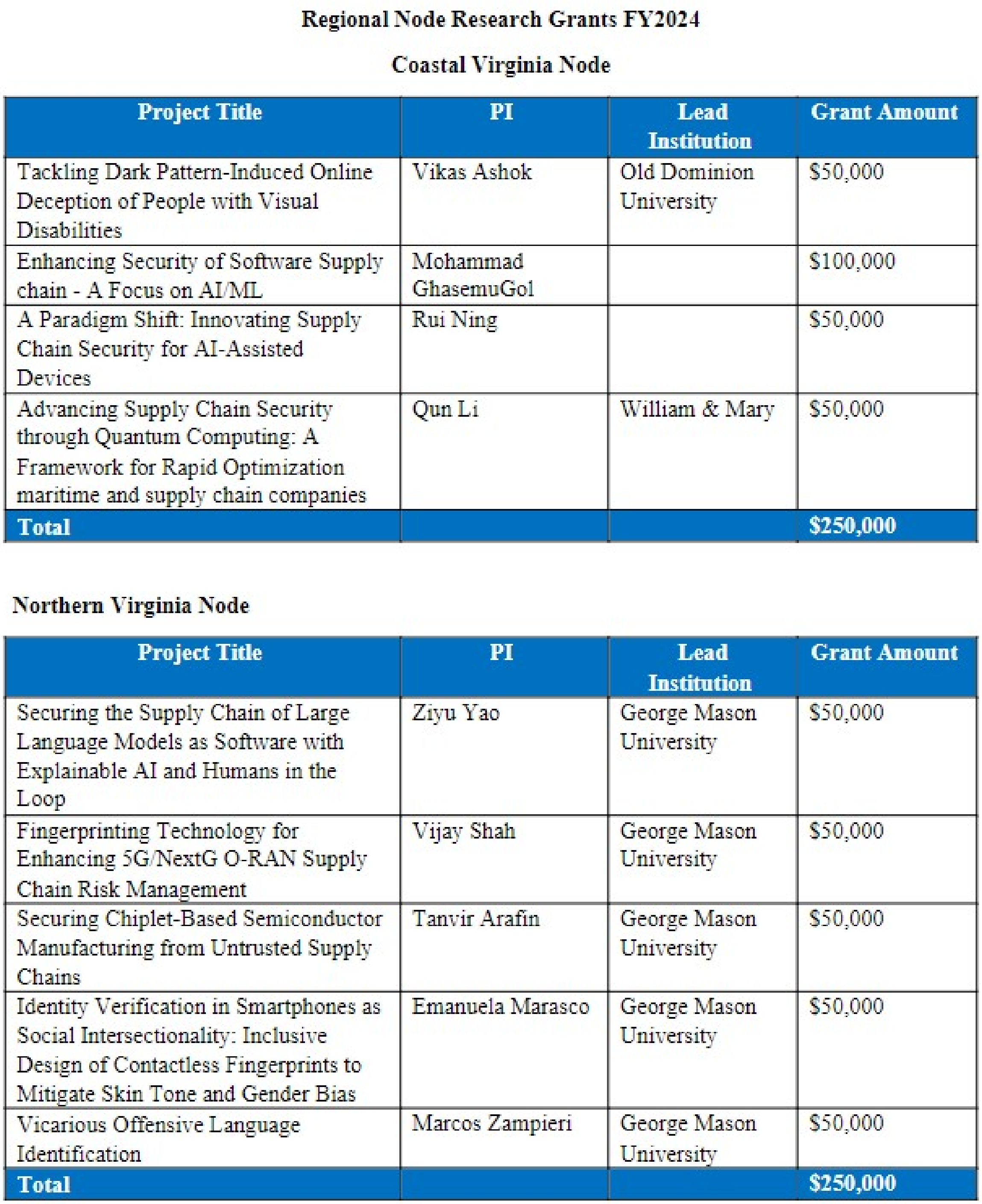
Central Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Building a Connected Future: Advancing OpenCyberCity for Collaborative Research, Education and Innovation	Sherif Abdelwahed	Virginia Commonwealth University	$100,000
Low resource Edge hardware Autoencoders for anomaly Detection in Smart cities networks (LEADS)	Jayasimha Atulasimha	Virginia Commonwealth University	$100,000
CRIPTAG - Computational RFID for Privacy and Trust in IoT Applications	Mircea R. Stan	University of Virginia	$100,000
Machine Learning based CAN Bus Data Attack Detection in Autonomous Vehicles	Haiying Shen	University of Virginia	$100,000
Low-cost and Long-lasting Soil Moisture Sensing with WiFi signals and Energy Harvesting	Eyuphan Bulut	Virginia Commonwealth University	$100,000
SafePath: Automated Extraction of Temporal Logic Based Trajectory Embeddings for Enhanced Autonomous Vehicle Safety.	Madhur Behl	University of Virginia	$100,000
Weakly-supervised Federated Graph Learning for Cyber-Physical Systems	Jungdong Li	University of Virginia	$100,000
Graph Neural Networks for Smart Infrastructure Systems with Large Number of Heterogeneous IoT Sensors	Negin Alemazoor	University of Virginia	$100,000
			$800,000

Figure 2.5: Central Node Research Grants Awarded for FY24.

Dr. Harpreet S. Dhillon, from VT, is a FY24 CCI fellow leading a project to launch the Institute for the Mathematics of Technology-Inspired Applications (IMTIA) through the prestigious NSF Mathematical Sciences Research Institutes program. Positioned to be a national resource for the mathematical sciences and adjacent communities, IMTIA will be a collaboration between VT and the University of Virginia that will grow into an international resource. It will be the first national institute to focus on mathematics for science and engineering applications prompted by the capabilities and challenges of a digital world. Dr. Dhillon and his team will seek diverse solicitations of interest, with a total budget goal of $20M-$30M over five years of performance.

Dr. Ross Gore from ODU leads, as a CCI fellow, a project titled ”Individualized and Effective Cyber Risk Training Using Large Language Models.” Dr. Gore’s project proposes a paradign shift in approaching communicating cybersecurity risks and conducting office training related to cybersecurity threats. The project team proposes a framework that can be applied to any type of cyber threat to generate individualized cyber risk communication and/or office training containing desired stakeholder information. These messages and training are more inclusive of their audience and produce a more directed educational/training response



Regional Node Research Grants FY2024

Coastal Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Tackling Dark Pattern-Induced Online Deception of People with Visual Disabilities	Vikas Ashok	Old Dominion University	$50,000
Enhancing Security of Software Supply chain - A Focus on AI/ML	Mohammad GhasemuGol		$100,000
A Paradigm Shift: Innovating Supply Chain Security for AI-Assisted Devices	Rui Ning		$50,000
Advancing Supply Chain Security through Quantum Computing: A Framework for Rapid Optimization maritime and supply chain companies	Qun Li	William & Mary	$50,000
Total			**$250,000**

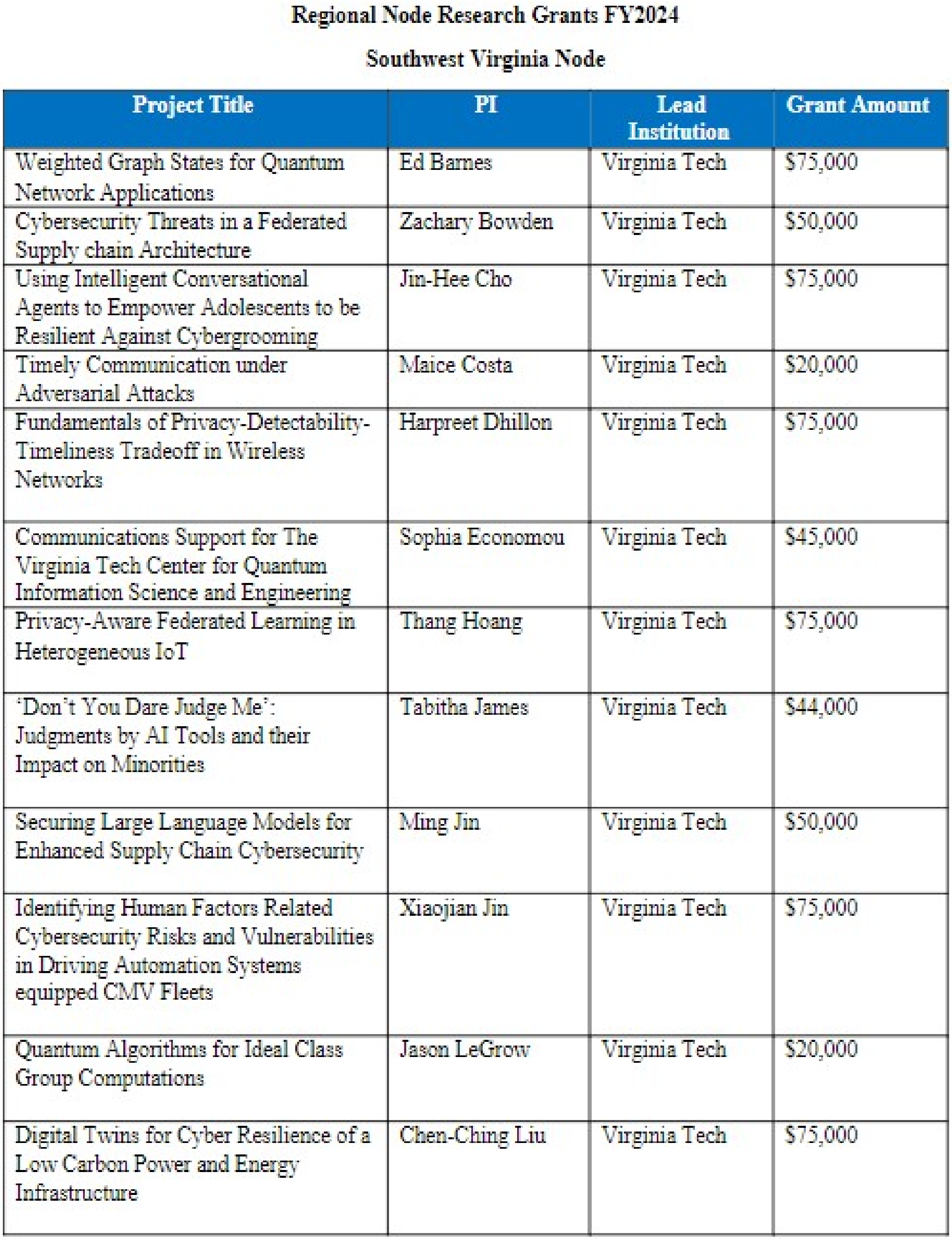
Northern Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Securing the Supply Chain of Large Language Models as Software with Explainable AI and Humans in the Loop	Ziyu Yao	George Mason University	$50,000
Fingerprinting Technology for Enhancing 5G/NextG O-RAN Supply Chain Risk Management	Vijay Shah	George Mason University	$50,000
Securing Chiplet-Based Semiconductor Manufacturing from Untrusted Supply Chains	Tanvir Arafin	George Mason University	$50,000
Identity Verification in Smartphones as Social Intersectionality: Inclusive Design of Contactless Fingerprints to Mitigate Skin Tone and Gender Bias	Emanuela Marasco	George Mason University	$50,000
Vicarious Offensive Language Identification	Marcos Zampieri	George Mason University	$50,000
Total			**$250,000**

Figure 2.6: Coastal and NoVA Node Research Grants Awarded for FY24.

because they are individualised using large language models (i.e., ChatGPT, BERT, Claude, Ernie, Falcon, Lambda, etc.). This approach will be described in a proposal submitted to the NSF Computer and Information Science and Engineering (CISE) Core Programs, Large Projects Opportunity with a total budget of $4M in collaboration with VT, Mason, and William and Mary.

Dr. Parth Pathak, a FY24 fellow from Mason, is leading a project titled ”Open-Milli-IoT: An Open



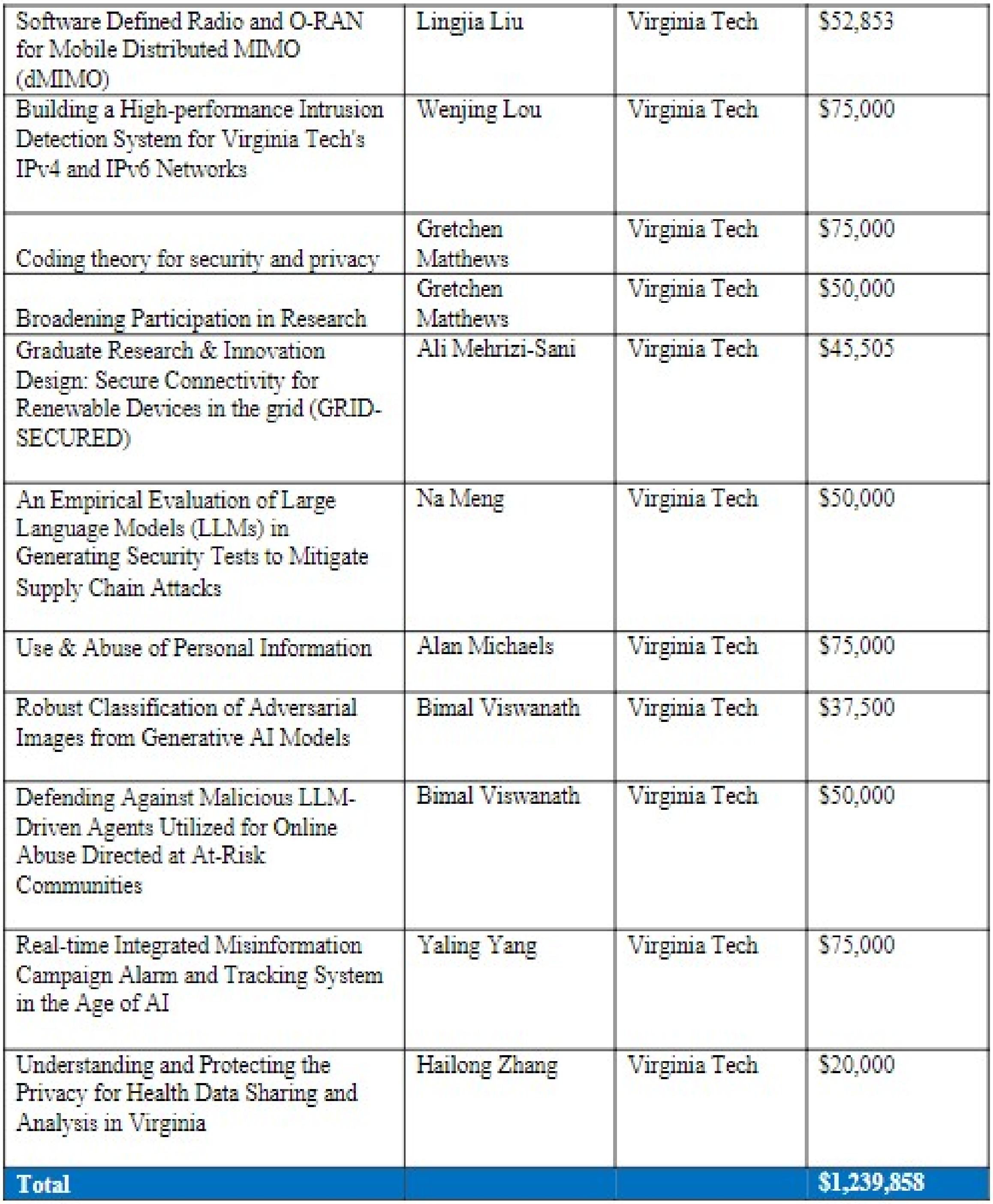
Regional Node Research Grants FY2024

Southwest Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Weighted Graph States for Quantum Network Applications	Ed Barnes	Virginia Tech	$75,000
Cybersecurity Threats in a Federated Supply chain Architecture	Zachary Bowden	Virginia Tech	$50,000
Using Intelligent Conversational Agents to Empower Adolescents to be Resilient Against Cybergrooming	Jin-Hee Cho	Virginia Tech	$75,000
Timely Communication under Adversarial Attacks	Maice Costa	Virginia Tech	$20,000
Fundamentals of Privacy-Detectability-Timeliness Tradeoff in Wireless Networks	Harpreet Dhillon	Virginia Tech	$75,000
Communications Support for The Virginia Tech Center for Quantum Information Science and Engineering	Sophia Economou	Virginia Tech	$45,000
Privacy-Aware Federated Learning in Heterogeneous IoT	Thang Hoang	Virginia Tech	$75,000
'Don't You Dare Judge Me': Judgments by AI Tools and their Impact on Minorities	Tabitha James	Virginia Tech	$44,000
Securing Large Language Models for Enhanced Supply Chain Cybersecurity	Ming Jin	Virginia Tech	$50,000
Identifying Human Factors Related Cybersecurity Risks and Vulnerabilities in Driving Automation Systems equipped CMV Fleets	Xiaojian Jin	Virginia Tech	$75,000
Quantum Algorithms for Ideal Class Group Computations	Jason LeGrow	Virginia Tech	$20,000
Digital Twins for Cyber Resilience of a Low Carbon Power and Energy Infrastructure	Chen-Ching Liu	Virginia Tech	$75,000

Figure 2.7: Southwest Node Research Grants Awarded for FY24.

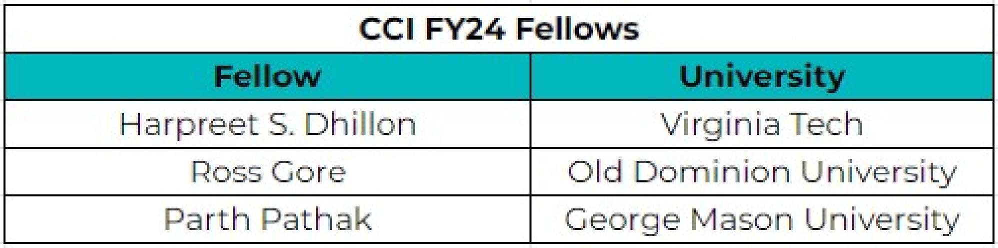
Programmable Platform for mmWave Wireless Internet-of-Things" with VT. The vision for the proposal is to develop a first-of-its-kind research platform titled Open-Milli-IoT for investigating and developing mmWave



Software Defined Radio and O-RAN for Mobile Distributed MIMO (dMIMO)	Lingjia Liu	Virginia Tech	$52,853
Building a High-performance Intrusion Detection System for Virginia Tech's IPv4 and IPv6 Networks	Wenjing Lou	Virginia Tech	$75,000
Coding theory for security and privacy	Gretchen Matthews	Virginia Tech	$75,000
Broadening Participation in Research	Gretchen Matthews	Virginia Tech	$50,000
Graduate Research & Innovation Design: Secure Connectivity for Renewable Devices in the grid (GRID-SECURED)	Ali Mehrizi-Sani	Virginia Tech	$45,505
An Empirical Evaluation of Large Language Models (LLMs) in Generating Security Tests to Mitigate Supply Chain Attacks	Na Meng	Virginia Tech	$50,000
Use & Abuse of Personal Information	Alan Michaels	Virginia Tech	$75,000
Robust Classification of Adversarial Images from Generative AI Models	Bimal Viswanath	Virginia Tech	$37,500
Defending Against Malicious LLM-Driven Agents Utilized for Online Abuse Directed at At-Risk Communities	Bimal Viswanath	Virginia Tech	$50,000
Real-time Integrated Misinformation Campaign Alarm and Tracking System in the Age of AI	Yaling Yang	Virginia Tech	$75,000
Understanding and Protecting the Privacy for Health Data Sharing and Analysis in Virginia	Hailong Zhang	Virginia Tech	$20,000
Total			**$1,239,858**

Figure 2.8: Southwest Node Research Grants Awarded for FY24.

IoTs. This project aims to jointly orchestrate and manage mmWave communication and IoT devices through programmable and intelligent radio networks in the form of Open RAN. The research framework will have three key components to produce ultra-high localization accuracy, ultra-low latency at extremely low power consumption, intelligent and robust networking protocols to enable communication with mmWave IoTs, as well as provide agility and flexibility for mmWave IoT devices so that RIS and conventional clients and base stations can be seamlessly integrated, orchestrated, and managed as a unified architecture. Dr. Pathak and his team aim to develop a large center-scale proposal for the NSF CCRI (CISE Community Research Infrastructure) and/or NSF MRI (Major Research Instrumentation) opportunities, with at least a $2M anticipated budget.



CCI FY24 Fellows	
Fellow	**University**
Harpreet S. Dhillon	Virginia Tech
Ross Gore	Old Dominion University
Parth Pathak	George Mason University

Figure 2.9: CCI Fellows FY24.

2.3 Faculty Recruited

2.3.1 Hub Faculty

The CCI Hub hired one post-doctoral researcher in FY24:

Dr. Pratiti Paul (Figure 2.10) is currently a Presidential Postdoctoral Fellow at the CCI Hub at VT Arlington Research Center in Arlington, Virginia. Before joining VT, Dr. Paul received her Ph.D. from the Indian Institute of Technology, Delhi (IIT Delhi) and worked as a Research Associate at the University of Edinburgh, UK. Her current research aims to contribute to developing resilient sixth-generation (6G) wireless systems, focusing on Vehicular-to-Vehicular Communication. The expected impact includes the development of a resilient 6G infrastructure, reliable wireless systems with efficient link design, advanced learning-based threat detection, and mitigation of such adverse events. The multi-disciplinary research draws from communication theory, machine learning, security, and statistics, with a focus on building a resilient and secure 6G system. Dr. Paul currently serves as a technical reviewer for IEEE Transactions on Communication and IETE Journal of Research, and is a technical instructor in the IIT Delhi Certificate Programme in ”Machine Learning and Deep Learning.”

Figure 2.10: Dr. Pratiti Paul.

2.3.2 Node Faculty

2.3.3 Northern Virginia Node

Dr. Matt Jablonski was recruited to George Mason University as part of a cluster hire with Old Dominion University. He will conduct research at George mason University and as part of the Northern Virginia Node of the Commonwealth Cyber Initiative, and in partnership with researchers from the Coastal Node of the Commonwealth Cyber Initiative and Old Dominion University. He and his counterparts at ODU will have access to the faculty and facilities of both universities to enable their success.

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

- Assisting in the interdisciplinary research effort between George mason University, Old Dominion University, and the Northern Virginia and Coastal Virginia nodes of CCI.
- Leverage university-level strategic priorities in cybersecurity research to lead transformative growth and impact the research portfolio, and to further encourage and foster new and existing collaborations with academic, industrial, and governmental institutions in Northern Virginia, Coastal Virginia and the greater Washington D.C. area.
- Accelerate the growth of high-quality academic programs, facilitate interdisciplinary research initiatives, and broaden the scope and focus areas of research in Mason with significant potential for commercialization.

Dr. Jablonski received his Bachelor's degree in Computer Science from Virginia Tech, and his M.S. degree in Information Security and Assurance and a Ph.D. in Computer Science from George Mason University. Since 2019, he has served as Vice President of Security Research for B4Corp. Dr. Jablonski is active in CyMANII, SAE International, and IEEE. His research intersts include risk analysis, offensive and defensive operations, formal methods, cyber physical systems, networking and telecommunications, and reverse engineering.

2.3.4 Coastal Virginia Node

Dr. Daniel Takabi Takabi is the new Director of ODU's School of Cybersecurity, the new Coastal Node Director, as well as the Batten Endowed Chair of Cybersecurity and professor of electrical and computer engineering.

He previously served as founding director of the Information Security and Privacy: Interdisciplinary Research and Education (INSPIRE) Center at Georgia State University. He led efforts resulting in GSU's designation by the National Security Agency as a National Center of Academic Excellence in Cyber Research and a National Center of Academic Excellence in Cyber Defense. He also served as program director for the cybersecurity programs, managed the CyberCorps Scholarship for Service (SFS) program and developed the Graduate Certificate in Trustworthy AI Systems program at GSU.

At ODU, Dr. Takabi will collaborate on cybersecurity research and initiatives with units across campus, including the Center for Secure and Intelligent Critical Systems, led by Sachin Shetty, and the supply chain cybersecurity research led by Rafael Diaz. He will also work with other universities on cybersecurity research and will be an active participant in the Commonwealth Cyber Initiative.

Dr. Takabi's research focus is Cybersecurity and privacy, including the intersection of artificial intelligence (AI) and data science with cybersecurity and privacy; privacy-enhancing technologies; computation over encrypted data; and usable security and privacy.

Dr. Mohammad GhasemiGol is a research assistant professor at Old Dominion University's School of Cybersecurity.

He holds BS and MS degrees in Computer Engineering. For his Ph.D., he specialized in alert management and intrusion response systems. During his Ph.D. studies, he worked with the Information Security and Privacy: Interdisciplinary Research and Education (INSPIRE) group at the University of North Texas (UNT).

Before joining ODU, he was at the University of Birjand (UoB) as an assistant professor in the department of computer engineering. He was also the director of the Computer Emergency Readiness Team (CERT) and director of Information Communication and Technology (ICT) at UoB for more than 4 years. He later joined Imperial College London as an associate researcher in the Resilient Information Systems Security (RISS) Group, as a part of cyber security competence for research and innovation (CONCORDIA) project. After that, he was a research assistant professor in the University of North Dakota's College of Engineering & Mines.

Dr. Robert Podschwadt is a Research Assistant Professor in the School Cybersecurity of Old Dominion University. He earned his Ph.D. in Computer Science from Georgia State University in 2024. He has as B.S. and M.S. in Computer Science from Hochschule der Medien Stuttgart (Stuttgart Media University), Germany. From 2012 to 2017, he worked as a System Developer for Rhode & Schwarz Cybersecurity. His research focuses on security and privacy in machine learning and applications of machine learning for security critical tasks. He studies the use of privacy enhancing technologies like homomorphic encryption and secure multi-party computation for privacy preservation in machine learning. He is also interested in security applications of machine learning, and in adversarial examples.

Dr. Neda Moghim is a research assistant professor at Old Dominion's School of Cybersecurity, who originally joined ODU in the Virginia Modeling, Analysis, and Simulation Center.

Previously, she was an associate professor in the University of Isfahan's Department of Computer Engineering. She holds a PhD and M.Sc. in Communication Systems Engineering, and a B.Sc. in Electrical Engineering. She is the author of several technical papers in telecommunications journals and conferences.

Md Shirajum Munir is a research assistant professor at Old Dominion University's School of Cyber Security.

Previously, he served as a post-doctoral research associate at ODU's Virginia Modeling, Analysis, and Simulation Center. Before joining ODU, he was a postdoctoral researcher at Kyung Hee University's Department of Computer Science and Engineering.

He holds a B.S. in Computer Science and Engineering and a Ph.D. in Computer Engineering. He has also worked in software engineering at the Samsung Research and Development Institute. He's published in IEEE journals and presented at IEEE and other conferences. He's a member of IEEE, IEEE Communication Society, IEEE Young Professional, and The Institution of Engineers, Bangladesh (IEB).

2.3.5 Southwest Virginia Node

Dr. Atul Mantri was recruited from the University of Maryland, where he was a postdoctoral associate. Previously, he was a postdoctoral associate at University of Edinburgh. His research expertise is rooted in the burgeoning field of quantum computation and quantum information, with a specific focus on quantum cryptography. His work involves the application of cryptographic methodologies to construct secure protocols in the quantum domain, as well as the design of classical cryptographic protocols resilient against the computational capabilities of quantum computers. Atul received his doctorate from Center for Quantum Technologies (CQT), National University of Singapore and Singapore University of Technology and Design in 2019.

Dr. Emily McMillon is a Virginia Tech Presidential Postdoctoral Fellow and NSF Postdoctoral Fellow in the Mathematics Department at Virginia Tech.

Dr. Emily McMillon was recruited from Rice University, where she was an NSF Postdoctoral Fellow. She earned her doctorate in Mathematics from the University of Nebraska-Lincoln. Her research interests are coding theory and applied discrete mathematics. She is specifically interested in graph-based codes and iterative decoder analysis.

Dr. Sangmork Park is an assistant computer science and information science professor at VMI. He received a Ph.D. from the Wright State University in Dayton, Ohio, and a master's degree from the Air Force Institute of Technology at Wright-Patt AFB. His research interests include cybersecurity, machine learning, cloud computing, C4I systems, simulation, and optimization.

2.3.6 Central Virginia Node

The Central Virginia Node did not recruit new faculty members in FY24.

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 FY24, CCI's xG testbed has continued to expand, with the beginning of our outdoor deployment in Blacksburg, VA.

Value Proposition

The xG Testbed contains assets for research and innovation in 5G and NextG, embedding Artificial Intelligence (AI) in the operation of the network, supporting research in network security, O-RAN security, and AI assurance, among other topics. Figure 2.11 shows the logo developed for the testbed.

Figure 2.11: CCI xG Testbed logo.

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

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

Design Principles

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

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

- Flexibility: flexible network management and orchestration compliant with an end-to-end 5G architecture composed of a mix and match of open-source and commercial hardware and software, with a cybersecurity focus, enabling indoor and outdoor deployment;

- Componentization: fully componentized implementation with open Application Programming Interfaces (APIs); containerized, cloud-ready implementations;

- Interoperability: integration ensuring the integrity of the end-to-end solution; interoperability among network components and existing testbeds, securing and hardening the network infrastructure;

- Support of verticals: alignment with key verticals to be supported by 5G and Next G networks, and co-location with research infrastructure supporting those verticals.

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

2.5 Research Highlights and Breakthroughs

CCI is presenting some of our researchers' exciting work through selected papers that have been presented, published, or accepted for publication in 2023 and 2024.

Submissions came from CCI researchers at George Mason University, James Madison University, Old Dominion University, Virginia Commonwealth University, Virginia Tech, and William and Mary.

Learn more about all the selected papers as well as papers of note.

Many papers were the product of collaborations between researchers at multiple CCI member universities, as well as institutions in other states and nations. Papers are focused on cybersecurity, have benefited from CCI funding, and acknowledge CCI's contribution in the publication/presentation. They include:

Horizontal Gaze Nystagmus Transmission Interlock System: Building a personalized machine-learning algorithm calibrated to test drivers' sobriety while protecting their privacy. Authors: Chase Coleman, Matthew Jenkins, William Roberts, Charlie Thomas, William, Westerkamp, Rod MacDonald, Ahmad Salman

Strategic Resilience Evaluation of Neural Networks within Autonomous Vehicle Software: Exploring safety pitfalls of deep neural networks used in autonomic vehicles in the presence of transient hardware faults. Authors: Anna Schmedding, Philip Schowitz, Xugui Zhou, Yiyang Lu, Lishan Yang, Homa Alemzadeh, Evgenia Smirni

CANShield:Deep-Learning-Based Intrusion Detection Framework for Controller Area Networks at the Signal Level: Developing the CANShield to protect controller area network (CAN) bus from injection attacks. Authors: Md Hasan Shahriar, Yang Xiao, Pablo Moriano, Y. Thomas Hou, Wenjing Lou

A Zero Trust Framework for Realization and Defense Against Generative AI Attacks in Power Grid: Using a novel zero trust framework to recognize and protect against attack vectors. Authors: Md Shirajum Munir, Sravanthi Proddatoori, Manjushree Muralidhara, Walid Saad, Zhu Han, Sachin Shetty

A Machine Learning-Based Temperature Control Security Against FDI Attacks in Smart Buildings: Incorporating machine learning-driven anomaly detection into control systems for optimal indoor climate regulation. Authors: Mostafa Zaman, Maher Al Islam, Nasibeh Zohrabi, Sherif Abdelwahed

Resilient Power Sharing in a 100% Inverter-Based Power System Under GPS Spoofing Attacks: Improving control algorithm accuracy by fortifying existing power grid controllers against cyberattacks. Authors: Brady Alexander, Ardavan Mohammadhassani, Ali Mehrizi-Sani

P4CONTROL: Line-Rate Cross-Host Attack Prevention via In-Network Information Flow Control Enabled by Programmable Switches and eBPF: Leveraging programmable data to enforce information flow control at the network-level, using network infrastructure to block sophisticated attackers. Authors: Osama Bajaber, Bo Ji, Peng Gao

Malicious RIS vs. Massive MIMO: Securing Multiple Access Against RIS-Based Jamming Attacks: Developing an algorithm to optimize RIS reflection coefficients without knowing legitimate user channels. Authors: Arthur Sousa de Sena, Jacek Kibiłda, Nurul Huda Mahmood, André Gomes, Matti Latva-aho

Probing Weaknesses in GPU Reliability Assessment: A Cross-Layer Approach: Conducting a characterization study with extensive fault injection experiments on GPU applications to protect vulnerable systems. Authors: Lishan Yang, George Papadimitriou, Dimitrios Sartzetakis, Adwait Jog, Evgenia Smirni, Dimitris Gizopoulos

OSINT Research Studios: A Flexible Crowdsourcing Framework to Scale Up Open Source Intelligence Investigations: Developing a sociotechnical framework to provide training and scaffolding to support OSINT investigations. Authors: Anirban Mukhopadhyay, Sukrit Venkatagiri, Kurt Luther

SOK: Side Channel Monitoring for Additive Manufacturing - Bridging Cybersecurity and Quality Assurance Communities: Consolidating and systemizing knowledge to explore SCs in additive manufacturing while highlighting QA and cybersecurity communities' collaboration opportunities. Authors: Muhammad Ahsan, Muhammad Haris Rais, Irfan Ahmed

An Analysis of Recent Advances in Deepfake Image Detection in an Evolving Threat Landscape: Developing concrete and specific future work directions to build resilient and reliable deepfake detectors. Authors: Sifat Muhammad Abdullah, Aravind Cheruvu, Shravya Kanchi, Taejoong (Tijay) Chung, Peng Gao, Bimal Viswanath, Murtuza Jadliwala

2.5.1 Highlight: The CHIPS and Science Act and O-RAN

The Public Supply Chain Wireless Innovation Fund is a $1.5 billion program that supports the development of open wireless networks. A key objective is to lower the barrier to entry for new vendors in the wireless supply chain, thereby spurring innovation. The program is funded under the CHIPS and Science Act and is managed and led by the NTIA.

The achievement of the program's objectives will have major economic development and national security implications. O-RAN's goal of intelligent, open, virtualized and fully interoperable mobile networks promises to spur marketplace competition and evolve network technology at a faster pace than proprietary or "black box" technology.

In FY24, the NTIA issued a Notice of Funding Opportunity (NOFO) for research and testing of innovative solutions in O-RAN. This call for proposals consisted of two tracks: research & development (R&D), and testing & experimentation (T&E). Hundreds of institutions responded to the call, and after judicious selection the NTIA awarded approximately $140 million to the projects selected for funding.

CCI researchers were extraordinarily successful under this call. The projects selected for funding included:

- Developing a holistic cybersecurity framework. Lead: Virginia Tech. Track: R&D. Total: $2 million.
- AI-Enabled efficient testing and evaluation for RU, DU, and CU components of 5G Radio Access Networks. Lead: Michigan State University. Participant: George Mason University. Track: R&D. Total: $1.7 million.
- Learning-based O-RAN testing. Lead: Virginia Tech. Track: R&D. Total: $2 million.
- Defense against sophisticated threats. Lead: Booz Allen Hamilton. Participant: Virginia Tech. Track: R&D. Total: $2 million.
- Digital twin to predict system failures. Lead: Cyrrus360. Participant: Virginia Tech. Track: R&D. Total: $2 million.
- Acceleration of commercialization and compatibility of O-RAN deployments. Leads: AT&T and Verizon. Participant: Virginia Tech. Track: T&E. Total: $42 million.

This success is the result of early investments by CCI in research infrastructure and personnel across multiple institutions. The CCI xG Testbed was designated an Open Testing and Integration Center (OTIC) by the O-RAN Alliance in 2023, recognizing our unique capabilities in research, testing, and experimentation with O-RAN solutions.

Becoming an O-RAN testing and integration center aligns with our mission to spur innovation, integrate security, and lower barriers to entry in the wireless market. CCI's investment in shared infrastructure gives industry partners and researchers across our network of more than 40 Virginia universities and colleges access to this crucial resource that will help build secure, fast networks. OTICs help achieve that goal by allowing vendors and providers to test, evaluate, and verify their products and software solutions.

In FY25 we will continue to be competitive in further funding opportunities announced by the NTIA.

Chapter 3

CCI Workforce Development

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

3.1 Hub-Led Programs

3.1.1 CCI Internship Fair

The CCI Internship Fair took place in late September 2023 and proves again to be one of our most popular programs. Over 500 students registered for this free and virtual event comprising a career panel featuring representatives from CACI and Expedition Technology, and employer booths. Nineteen employers participated ranging from government agencies to small Virginia-based companies. Featured employers included: CACI, Microsoft, G2Ops, and The U.S. Department of Health and Human Services.

3.1.2 CyberFusion

The Commonwealth Cyber Fusion, hosted by Virginia Military Institute (VMI), Senator Mark R. Warner, the Virginia Cyber Range, and CCI took place on the VMI campus on February 23-24, 2024. 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, career panel, and the Virginia Cup Capture the Flag Competition. The event hosted two competitions, one for 4-year and one for 2-year colleges. 150 students from 21 colleges and universities competed over the weekend. Friday's activities included a keynote speech by Oki Mek, Microsoft chief information security officer for the Federal Civilian Sector, and a veteran with a 20-year career inside the federal government; a job fair; an employer panel discussion regarding real-world advice for students; and a faculty/industry round table discussion hosted by representatives from the Commonwealth Cyber Initiative. This year's competition included 44 challenges, the most ever for this competition. The winners of the capture-the-flag-style Virginia Cyber Cup competition for the four-year college division are: George Mason University in first, University of Virginia finishing second, and Virginia Tech in third. For the community college division: Tidewater Community College was the winner, followed by Northern Virginia Community College in second, and Virginia Western Community College in third. George Mason University was the overall winner and received the Commonwealth Cyber Fusion Cup.

3.1.3 Project-based Learning Program

The CCI Project-Based Learning Program solicits projects from industry sponsors for students to work on for one or two semesters while being actively mentored by the industry sponsor. Our first pilot project was with CACI and Northern Virginia Community College (NVCC). CACI accepted seven cyber students from NVCC, who worked on two discrete projects for two semesters. CCI paid the students' stipend and monitored the projects. In FY24 CACI decided to accept another cohort of students, this time selected from schools across the commonwealth. Additionally, Microsoft has joined the program and has accepted two cohorts to work on two separate projects. The first project, Flipper Zero Research, has provided students a flipper zero device on which to conduct research over the course of the summer. Students will present their research projects to MS employees at a company-wide lunch and learn event. The second project is hosted by Microsoft Federal: students will work with Microsoft Cloud and Cybersecurity subject matter experts (SMEs) to build a simulated enterprise cloud environment to conduct cybersecurity operations. Students will learn about modern cloud environments and cloud-focused cybersecurity operations to enhance their studies, gain work experience, and add to their skills in cloud-based technologies.

3.1.4 Clearance Preparedness Program

In FY24 the CCI Hub continued a virtual series to prepare students for the security clearance process, after a successful initial cohort in FY23 with over 400 students registering. This program, entitled ”The Clearance Preparedness Program” includes ten virtual webinars ranging in topics from ”What is a security clearance and why would I want one?” to ”Common reasons people do not pass a clearance process”. Students from across CCI are eligible to participate and if they attend 80 percent of the modules, they will earn a digital badge signaling that they are informed about and prepared to begin a security clearance process. The modules are hosted by CCI's Dr. Eric Burger and feature representatives from industry and government discussing various aspects of security clearances.

3.1.5 Experiential Learning Program in FY24

The Experiential Learning Program is CCI's longest running program, with the FY24 batch of awards being the fifth time CCI has run this program. Over the past five years CCI has awarded 36 proposals totaling in $3,932,392.00 in funding (Figure 3.1). With each project engaging anywhere from 10 to 25 students, this program has impacted hundreds of students across the state.

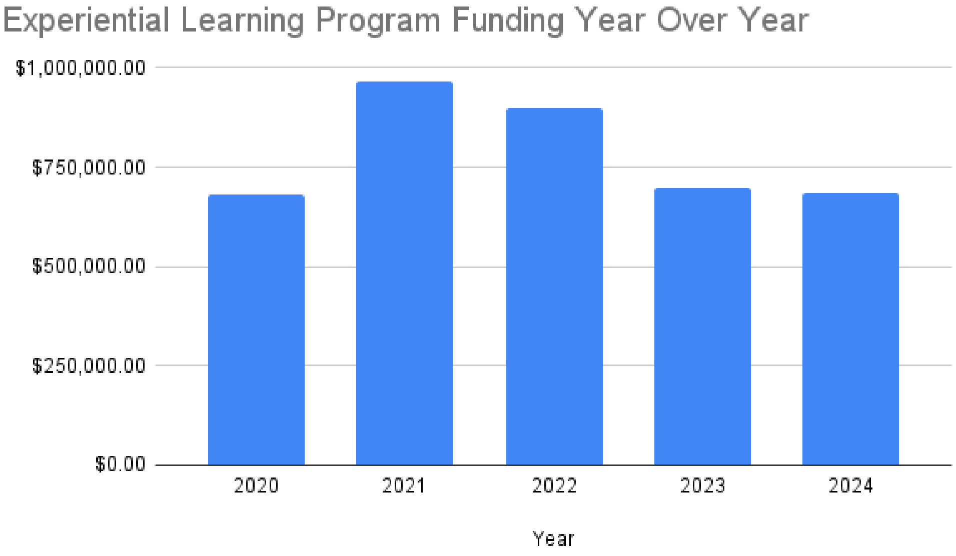


Figure 3.1: Experiential Learning Program Funding Year Over Year.

In its fifth iteration, the 2024 Experiential Learning call for proposals elicited 16 submissions, with seven successful proposals totalling $684,099 awarded in grants. CCI researchers were eligible to respond to this call, and proposals were selected based on recommendations by a peer review group. The percentage of the funding for projects in each CCI Node is shown in Figure 3.2.

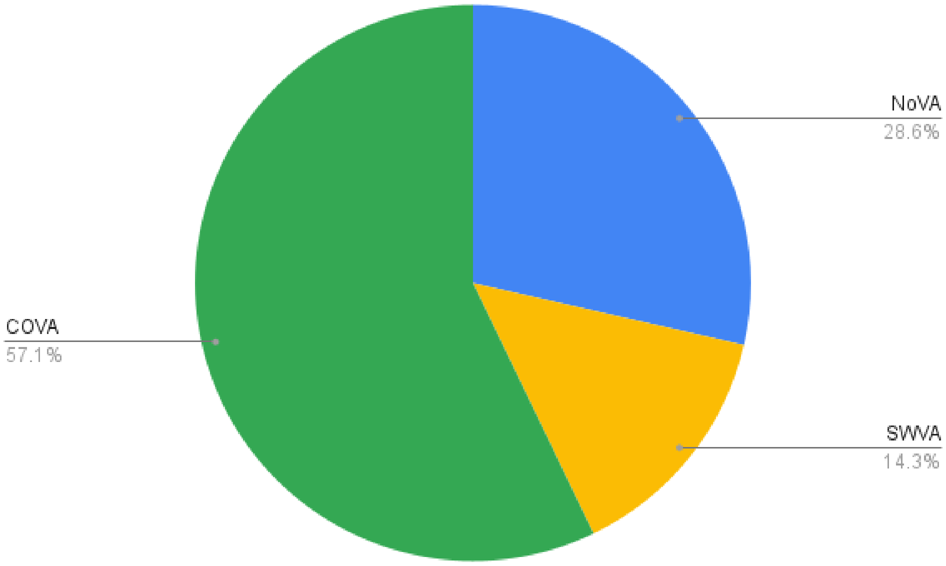


Figure 3.2: Funding percentage by Node for the FY24 Experiential Learning program.

The projects funded by this program are summarized below.

- **Mobile Security (Andriod) through Experiential Learning**: Yanhai Xiong W&M, Kun Sun, Mason; $84,099. As of March 2024, Android commands almost 71 percent of the global smartphone market. Android is also increasingly being utilized in emerging IoT and wearable devices. The Android operating system presents significant cybersecurity challenges as attackers seek to exploit the platform for financial gain. Researchers plan to: Equip students with foundational and advanced knowledge and skills in Android security; Foster practical problem-solving capabilities through direct collaboration with industry leaders such as Google and Visa; Enhance communication and cooperative skills through cross-university teamwork and partnerships between academia and industry; Facilitates immediate professional pathways for students by collaborating with industry giants like Google and Visa.

- **Cyber Startups**: Gisele Stoltz; Mason; $100,000. Building on seven semester-long cohorts of CCI Experiential Learning Programs, the proposal will set up internships that offer George Mason University's micro-credential certification to students from Mason and other students from NoVA Node schools, which can be added to LinkedIn profiles as a certified qualification of tech entrepreneurship. The program will match students from Mason and other NoVA Node schools, including transfers from regional community colleges, with local cybersecurity startups and subject matter experts. Interns will supplement this experience with a tech-focused entrepreneurship curriculum. The semester-long program will be offered twice a year, in the Spring and Fall, aiming to place 50 students per year.

- **Intelligent Automation for Cyber Ready Industrial Control Systems Training Program for Safe and Secure Shipbuilding Operations**: Sachin Shetty, ODU; Md Shirajum Munir ODU; Le Thanh Tan, Hampton University; $100,000. Secure Industry Control Systems (SICS) have a tremendous impact in commercial, government, and military sectors due to advances in machine learning, Internet of Things, and autonomy technologies. The shipbuilding industry needs efficient methods to protect sensitive data and prevent malicious attacks. Another challenge is ensuring the security of cyber-infrastructure within interconnected systems that improve operational efficiency but increase potential entry points for attacks. Successful cyber-attacks on processes underpinning ICS can create severe disruptions in all aspects of shipbuilding operations.

- **Automated Threat-Hunting System Development Learning Program**: Mohamed Gebril, Mason; Dr. Sherif Abdelhamid, VMI $100,000. Ease-of-use, precision of outputs, correlation between systems, and clear communication channels are among the most frequently mentioned as problematic. When designing security programs, organizations are increasingly interested in the implementation of proactive solutions to satisfy security requirements. Threat hunting programs designed to analyze, test, monitor, and secure systems aim to satisfy this trend. Researchers will enhance threat hunt solutions through the use of open-source tools from a list of problem areas derived from a set of interviews concerning the topic conducted during a previous CCI funded project. They will establish a basis for tool functionality and use continuous development and integration testing to provide a learning experience that simulates the real world. This initiative not only aims to enhance cybersecurity protocols through real-time network traffic monitoring and incident response but also to cultivate a skilled workforce adept at navigating the complexities of network security. The system developed through this program will be integrated into workshops hosted at Mason and VMI, with the added goal of serving the surrounding communities.

- **Expanding Experiential Learning Through the Commonwealth STEM Industry Internship Program Commonwealth STEM Industry Internship Program (CSIIP)**: Chris Carter; Virginia Space Grant Consortium (VSGC); $100,000. This partnership serves the entire Commonwealth and supports CCI's goal of cybersecurity workforce development. VSGC established CSIIP to support education, workforce development, and research by providing Virginia undergraduate students majoring in STEM with meaningful paid internships. The program is free to companies, schools, and students. CSIIP helps students explore career goals, apply classroom theory in the workplace, and develop their skills while working on real-world projects mentored by industry professionals. Since 2013, VSGC has placed more than 1,150 students, and several companies have hired their interns as full-time employees, including: Sentara; AScIS; Hampton Roads Sanitation District; RecAccess; Dominion Resource Services; MI Technical Solutions; BASF; York County; and City of Newport News.

- **Enhancing Experiential Learning via Technology Enabled Internships with Mentoring (TEIM)**; Jeff Pittges, Radford; Deri Draper-Amason, ODU; Milos Manic, VCU; Bobby Keener, Civilian Cyber CEO/CIO; $100,000. Employer surveys routinely show that students graduating from traditional programs aren't workforce-ready due to a lack of critical thinking/soft skills and the inability to apply theoretical knowledge learned in the classroom. While experiential learning approaches seek to address this issue, many lack needed structure. The CCI-aligned TEEM program has previously served more than 150 students from 12 CCI-affiliated institutions of higher education and 13 school divisions, with more than 75 industry professionals acting as mentors. TEEM will continue to leverage the successful approach of having experienced higher-education students serve as the mentors for less experienced college and high school students. This phase will also meaningfully enhance TEEM by: Developing a required student-mentor micro-credential aligned to mentoring best practices; Aligning the program to Virginia High Quality Work-Based Learning (HQWBL) requirements; Funding the proposal will drive 45 mentor/mentee student engagements representing institutions throughout Virginia.

3.1.6 Cyber As A Service

In FY24, the CCI Hub began a new program called Cyber As a Service in which projects, performed primarily by students, provide a cyber service (e.g., penetration or pen testing, cyber risk analysis) to Virginia small businesses or not-for-profits in the same county as the institution of higher education. This in an ongoing call for proposals with maximum grant awards of $15,000. One such project funded through UVA Wise, called the Exploration of CyberSystem Risk in Wise County Small Businesses, will be student-centered having a two-prong focus on providing: (1) an authentic learning opportunity for students to work with a Wise County area small business in providing a cybersystem risk analysis producing a risk register documenting identified cyber risk scenarios plus mitigation analysis and (2) a service for the Wise County, Virginia, small businesses with the students' time and effort being compensated solely by the grant. The Kerckhoff principle provides the guiding force here as it is essential when designing systems to be secure and ensuring a small business customers' personal information protection (PIP) as well as the business's information utilized for day-to-day business practices and historical data for report production remains uncompromised. Cyber risk's omnipresence within rural areas is a priority for Wise County's local small business enhancing the need for a service to provide a cybersystem risk analysis.

3.2 Node-led Programs

In addition to the CCI-wide programs described above, in the past year the CCI Nodes also developed and executed many successful workforce programs. Workforce development spending by the four CCI Nodes totaled $1,669,000.00 in FY24. The breakdown by Node is shown in Figure 3.3.

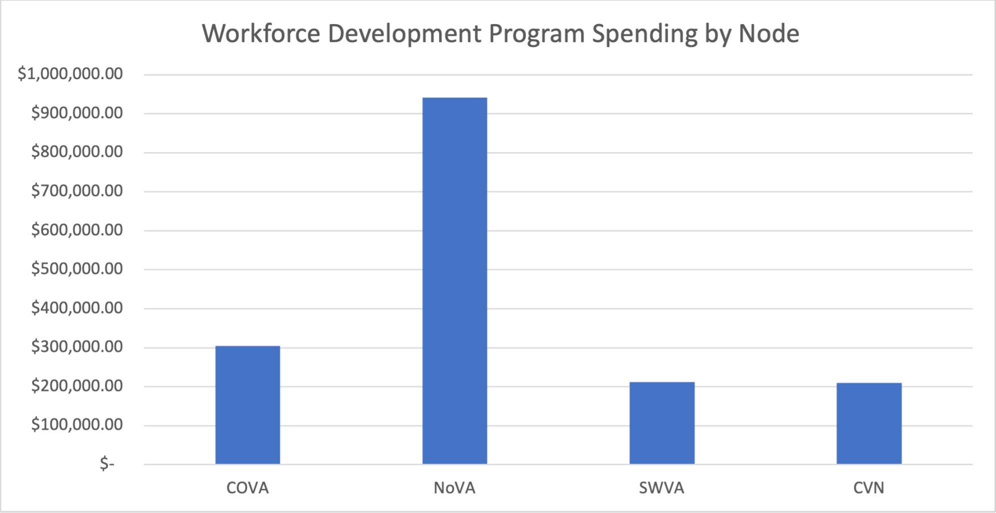


Figure 3.3: Workforce Development spending by Node in FY24.

3.2.1 NoVA Node

The NoVA Node carried out six workforce initiatives:

- **High School Cybersecurity Internship Program**: The CCI NoVA CCI NoVa Node is funding 40 high school students for internships with cybersecurity companies during Summer 2024. The experience includes a 2-week professional skills training program to prepare students for the professional work environment. 149 applications were received for the 40 available placements. Of the selected applicants, 47% identify as women or non-binary, and 57% come from underrepresented populations in science and engineering. Host companies include: Appian, Loudontec, Virginia Tech Thinkabit Physical Computing Lab, Chainbridge Solutions, Solvitur Systems, Maximus, Leidos, NT Concepts, Obscurity Labs, GT Cyber Labs, F1 Cloud Solutions, CGI Federal, and Widelity. This program is an expansion of the successful program launched in FY21 and scaled in FY22.

- **University/College Cybersecurity Entrepreneurship Internship Program**: To support both workforce development and early-stage cybersecurity startups who have limited resources, George Mason University conducted an expansion of its successful Cybersecurity Internship program, partnering with entrepreneurs and their early-stage companies to provide invaluable experiential learning opportunities to students. CCI NoVa Node ran two cohorts of cybersecurity internships with early-stage companies in fall 2023 and spring 2024. The program received over 600 applications for 50 spots during the two cohorts. Thirty percent (30%) of the interns were female and 68% identified as non-white. Host companies included: DataLock Consulting Group, KaDSci, Total Cyber Solutions, Solvitur Systems, Assursec, Auspex Labs, Gigasheet Inc, Looking Glass, SylLab Systems, Rimstorm, Karambit.AI, Corvus Labs, NowSecure, PropelGPS, CodeLock Inc, InterSec Inc, Valicyber, Cybermonic, Pistevo

Decision, Widelity, Colvin Run Networks, ITInfra, TidalCyber, Frontier Foundry, Blue Cloak, and RPProServices. This effort not only expands cybersecurity experiential learning, but augments the workforce to accelerate commercialization of cybersecurity technologies and the creation of new jobs in the sector.

- **Undergraduate Research Program** CCI NoVA Node sponsored 26 undergraduate students conducting cybersecurity research at George Mason University, James Madison University and University of Mary Washington. Example research projects included:

  - Security Assessment
  - Space/Terrestrial Networking
  - The Cyber Workforce Gap's Impact on Organizations
  - Securing the Internet of Things (IoT) using AI Technologies
  - Enhancing Authentication on the Web
  - Healthcare Organizations and their Reliance on Vendors/Cloud Systems
  - Computer Vision for Safety Applications in Advanced Manufacturing
  - Factory Cyberphysical System Security
  - A Hybrid Evidence-Based Approach to Detecting and Mitigating Election Misinformation
  - Regional Cybersecurity Ecosystems

  These experiences are building significant technical expertise and capacity in 10 undergraduates, making them particularly well trained for advanced work in industry and government. Twenty-six percent (26%) of this year's Undergraduate Research Assistants cohort identify as women, and 52% identify with underrepresented population groups in science and engineering.

- **Teacher Cybersecurity Professional Development Program**. 15 public school teachers from across the region, including Arlington, Alexandria, Fairfax, Prince William, and Loudoun counties, participated in a 5-month cohort entailing virtual cybersecurity workshops and other training opportunities over the course of the academic year. The overall goal was to help teachers build confidence in their knowledge of cybersecurity and support introduction of cybersecurity concepts into the classroom, regardless of grade level or subject matter. Topics addressed in the professional development workshops included:

  - Intro to Cybersecurity
  - Linux 101/ Intro to a Cyber Range
  - Linux 102 and Fun with Linux
  - Passwords/ Cracking Passwords
  - Malicious Links and Untrusted Sources
  - File Hashing
  - Backdoor Attacks
  - Simple Web Application Attacks
  - Advanced Web Application Attacks
  - Intro to IT Fundamentals
  - Intro to Networking
  - Cybersecurity Awareness for Elementary and Middle School
  - Cyber Society Overview
  - Overview of Cybersecurity Basics for k-5 Teachers
  - Overview of Cybersecurity Basics for 6-8 Teachers

Based on the success of this program, cyber.org developed a similar program, based on a cohort model of learning, splitting between K-8 and high school teachers, and scaled it nationally. Given this approach, participants in the CCI NoVa Node program joined the larger cohorts, allowing for broader exposure to unique perspectives and classroom strategies. Sessions continued to be facilitated by CCI Nova Node partner cyber.org. The program culminated in presentations by teachers of lesson plans they have developed for their specific classrooms and disciplines with impact to more than 1500 K-12 students.

- **Cybersecurity Apprenticeship 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 Apprenticeship program is providing cybersecurity training and an immersive apprenticeship for people who wish to transition into a career in cybersecurity but do not have prior experience. This program includes a 7-week classroom learning and training experience, beginning June 10, 2024, followed by a 12-week apprenticeship/traineeship with a cybersecurity company. The program received over 308 applications for 23 available positions. 48% of the cohort identify as female. Underrepresented population groups in science and engineering 11 comprise 83% of this cohort. Placement in apprenticeships is ongoing and includes, to date, apprenticeships with Peraton, Sedulous, Auspex Labs, Trewon Technologies, 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 28 students participating in this program, with more onboarding. Industry hosts include CGI Federal, Rohic, Frost Mountain LLC., Great Victory Legends., IvySys Technologies, TekScope, Auspex Labs, CyRisk, and RPRC. Thirty-two percent (32%) of this cohort identify as female and 57% identify with underrepresented population groups in science and engineering.

In addition to these dedicated programs, CCI NoVa Node enabled the widening of the talent pipeline through the support of external initiatives targeting high school students. In FY24, CCI NoVa Node again supported the CyberStart program. CyberStart, built by an expert team of cybersecurity professionals, gives students hand-on experience with real-world cybersecurity tasks and simulations that help them learn and develop the skills necessary to meet the critical need for cybersecurity professionals. Virginia had 26 students honored as Scholars with Honors and an additional 221 participants noted as Scholars. Students living within the geographical boundaries of NoVa Node comprised 15 (58%) of those recognized as Scholars with Honors and 136 (61.5%) of those recognized as Scholars.

CCI NoVa Node also supported CyberSlam 3.0, which brought together members of the Secret Service, Homeland Security, high school teachers, George Mason University faculty, and more than 600 hundred students from five counties and 22 high schools from the region to participate in a hands-on cybersecurity event. NoVa Node also served as a sponsor for PatriotHacks 2023, which attracted over 500 students to develop their technical capacity to address real-world problems presented by industry. Additionally, CCI NoVa Node is sponsoring University of Mary Washington's Summer Experience learning program for 15 high school students, focusing on cybersecurity and skills building, at University of Mary Washington, to be held in July 2024.

Jordan Mason, CCI NoVa Node's Program Manager, continues to serve on the commonwealth's Computer Science Education Advisory Board, thereby providing input to recommendations for Computer Science education standards for k-12 and perspective on 13 basic skills critical to the cybersecurity workforce of the future.

3.2.2 COVA CCI

CoVA CCI continues its support of workforce development, and student experiential learning through the graduate student experiential learning (CyberExL) program and the Cybersecurity Internship Clinic. CoVA CCI spent $305,000 in experiential learning funding in FY24.

- **Graduate student experiential learning program (CyberExL)**. CoVA CCI's graduate student experiential learning program is managed by Dr. Stephanie Blackmon, William and Mary School of Education. The program was rebranded as CyberExL in 2021 and the first cohort of graduate students started working with their respective organizations in January 2022. In FY 2023, sixteen students representing Norfolk State University, Old Dominion University, and William and Mary completed this program. Additional information can be found on the CoVA CCI/Talent Development and Experiential Learning Program website.

- **Cybersecurity Internship Clinic**. During the Spring 2024 semester, COVA CCI supported a pilot of our Cybersecurity Internship Clinic. Eight (8) students from Old Dominion University and two micro-businesses - a non-profit religious ministry and a government contractor - were selected for this pilot. We partnered with Valor Cybersecurity, a local cybersecurity business, which provided training and subject-matter expertise to the students as they prepared to complete the assessment of the client businesses. We also had a representative from CISA speak about the CISA Cybersecurity Performance Goals and how they can be used to support small businesses. This clinic provides pro bono cybersecurity-as-a-service to small businesses, non-profits, local government offices/agencies/board, and other organizations using selected students to assess the organization's cybersecurity preparedness and risk posture. The objective of this clinic is to provide cybersecurity awareness and services (education, risk management posture) to client organizations within Hampton Roads while providing an experiential learning opportunity for the students participating in the program as cybersecurity interns/consultants. Specifically, this clinic targets those client organizations that do not have a strong cyber presence and who can find value in gaining knowledge of cybersecurity through cybersecurity awareness and services. This is a 15-week program offered during the fall and spring academic semesters. During the program, students receive training on different cybersecurity modules, allowing them to interview client organizations during the middle part. The students work in teams under the supervision of ODU faculty. The team provide service to the client in one or more areas of cybersecurity network defense, cybersecurity policies and procedures, cybersecurity training for employees, cyber risk assessments, and/or cybersecurity best practices.

3.2.3 SWVA Node

The SWVA Node funded 3 workforce programs, with each funding several projects:

- **Program – FY24 Workforce**

  1. Title: (SGDT) Smart-built Gamified environment as an autonomous collaborative cybersecurity Digital-Twin facilitating user-behavior modeling in the presence of attacks PI: Mohamed Azab Lead Institution: Virginia Military Institute Co-PIs & Institution: Denis Gracanin, Stephanie Travis (VT) Funding Program: FY24 Workforce FY24 Funds: $8,476 Summary: In this proposal, we present a cybersecurity gamified digital-twin experimentation and exercise platform emulating large-scale distributed smart-built environments for user behavior modeling and investigation in attack and defense situations. We build on the existing collaboration between two Senior Military Colleges, Virginia Military Institute (VMI) and Virginia Tech (VT). The VMI and VT PIs have collaborated since 2019 on related research problems. VMI cadets and VT graduate/undergraduate students work together to support the PIs' research activities. High school students selected from Montgomery and/or Rockbridge counties will be recruited to work on the project. VT PI Gracanin is also an Adjunct Professor at the VMI Department of Computer and Information Sciences where he teaches capstone courses (CIS 480 and CIS 490). VT PI is also a member of the VMI CyDef Lab team. VT Co-PI Travis is at the VT National Security Institute (NSI) where VT PI Gracanin is an affiliate faculty. VMI PI is a member of graduate students committees at VT and a collaborator with the VT DVE lab, and NSI at VT. VMI PI is also a member of the VMI CyDef Lab team.

  2. Title: RUSecure CTF Contest: Expanding Access to Cyber Security Education PI: Joe Chase Lead Institution: Radford University Co-PIs & Institution: Prem Uppuluri (RU) Funding Program: FY24 Workforce FY24 Funds: $49,950 Summary:

  The RUSecure CTF Contest began in 2014 as part of an NSA MEPP Grant and with support from Cypherpath. The goal of the Contest was, and continues to be, to explore applying the just-in-time learning strategies developed for our on-campus cybersecurity programs to the introduction of cybersecurity topics in high schools and community colleges. The Contest has grown from 35 students from 4 schools in 2014 to an average of more than 1300 students per year representing more than 60 schools.

3. Title: Broadening Participation in Security PI: Gretchen Matthews Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce FY24 Funds: $50,000 Summary: This project will broaden the participation in cybersecurity education, research, workforce development, and innovation. It will connect people in related areas to enhance opportunities and build capacity, working to (1) identify target groups, (2) determine metrics for success, (3) create points of entry for engagement and participation, (4) generate increased participation in events and programming, and (5) strengthen relationships with stakeholders to broaden impact and reach. We aim to increase diversity in terms of gender, race, ethnicity, geographic origin throughout Southwest Virginia, socioeconomic background, levels of learning (middle school, high school, community college, 4-year intuitions), disciplines, thus expanding opportunities for research funding, furthering access to curriculum, diversifying the node student body and ultimately the cybersecurity workforce.

4. Title: Math Undergraduate Research Program PI: Gretchen Matthews Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce FY24 Funds: $5,000 Summary: This academic year undergraduate research experience is designed to engage students in real-world applications of mathematics relevant to cybersecurity. Exposure to real-world applications early in a student's career and experience doing undergraduate research have both been shown to increase the retention of STEM majors, and the presence of a peer support system improves a sense of belonging, self-efficacy, attitudes and can increase effort, performance, active participation, and influence individuals' careers. This undergraduate research program increases equity amongst students as all students have an opportunity to engage in research, not just those who happen to be invited. This experience provides avenues into the discipline for all, including those who may not be the most vocal in or most prepared for a course or appear to be the most confident (factors largely influenced by gender, race, and socioeconomic status). Mentored by faculty and postdocs, students work in teams to code-based cryptography, coding theory (error correction and erasure recovery), and secure distributed computing.

5. Title: Virginia Cybersecurity Education Conference Teacher Sponsorships PI: Dave Raymond Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce FY23 Funds: $3,642 Summary: The Virginia Cyber Range has built a strong user community in Virginia public high schools and colleges and we serve thousands of users in hundreds of Virginia schools each semester. Each year we host the Virginia Cybersecurity Education Conference, giving high school and college educators in the Commonwealth an opportunity to share ideas and continue to build the Virginia cybersecurity education ecosystem. This project will support high school teachers by covering registration and some travel expenses.

6. Title: HBCU Quantum Partnership PI: Wayne Scales Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce FY23 Funds: $25,000 Summary: These funds are encumbered to support a Historically Black College or University (HBCU) conference at Virginia Tech to promote partnerships. The conference will also establish partnerships in QISE enabled technologies in cybersecurity, communication systems, artificial intelligence, machine learning, computing, and sensing. These partnerships are being designed to expand the research capacity and workforce development at HBCUs in QISE and QISE enabled technologies which is a priority of the federal government and industry.

7. Title: Support for the Living Learning Community Securitas at Virginia Tech – focused on Cybersecurity PI: Node Project Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce FY24 Funds: $11,205 Summary: A cybersecurity focused Living Learning Community is an integral component to achieving the goal of producing cybersecurity professionals and business leaders. Securitas: The Cybersecurity Living-Learning Community at Virginia Tech is the result of a collaborative effort between the Pamplin College of Business (Pamplin), the Commonwealth Cyber Initiative Southwest Virginia (CCI SWVA), the Hume Center for National Security and Technology, and the office of Living-Learning Programs. The funds this year were used to support the start of the community and pay a portion of the newly hired Program Coordinator for the LLC.

8. Title: Support for Cyber Clubs at Node Institutions PI: Node Project Lead Institution: Virginia

Tech Co-PIs & Institution: None Funding Program: FY24 Workforce FY24 Funds: $1,000 Summary: Support was offered to all node institutions for the support of cyber clubs. Virginia Tech's Cyber Club was funded.

9. Title: Outreach for Innovation and Workforce PI: Node Project Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce/Innovation FY24 Funds: $13,308 Summary: Our Outreach costs include support for Innovation and Workforce programs. This includes support for the Virginia Cybersecurity Conference, sponsoring some Roanoke/Blacksburg Technology Council (RBTC) events, and supporting Node events like the Annual meeting, Graduate Student Summit and Student Researcher Showcase.

- **Program – FY24 Workforce & Industry Engagement Program**

  1. Title: The Cybersecurity, Privacy, and Ethics of Electroencephalography PI: Aaron Brantly Lead Institution: Virginia Tech Co-PIs & Institution: Nataliya Brantly (VT) Funding Program: FY24 Workforce & Industry Engagement FY23 Funds: $10,000 Summary: The project aims to build an EEG headset capable of translating brainwaves into recognizable speech patterns. By constructing an EEG device using 3D printing and programming software, the practicality of brain-to-speech conversion and preliminary insights into potential privacy concerns regarding a person's thoughts can be assessed. An evaluation of the capabilities and limitations of real-time EEG speech decoding will provide a foundation for ethical considerations surrounding advancements in neurotechnology and its use commercially and in medicine.

  2. Title: Understanding How Software Developers Secure User Interfaces in Rapid Release Environments PI: Chris Brown Lead Institution: Virginia Tech Co-PIs & Institution: none Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $10,000 Summary: The goal of the proposed work is to understand current practices and challenges for securing user interfaces in modern software. In particular, we will explore the following research question: How do software developers secure user interfaces in rapid release environments? To answer this question, we will conduct a series of research activities to investigate GUI testing for security in CI/CD projects and the challenges therein.

  3. Title: Moving Target Defense for Time-Sensitive Cyber-Physical Systems (CPS) PI: Thidapat Chantem Lead Institution: Virginia Tech Co-PIs & Institution: Mohamed Azab (VMI) Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $10,000 Summary: In this project, we will use moving target defense (MTD) to secure RT-CPS. Specifically, we will implement MTD through hardware redundancy and configuration diversity. This will permit cross-layer awareness and strategic guidance to fortify system security against evolving threats. By incorporating hardware redundancy, the approach enables an RT-CPS to maintain operational integrity and meet deadline requirements even when specific components are compromised, while configuration diversity ensures that the system's setup varies over time or in response to detected threats, making it more difficult for attackers to exploit known vulnerabilities. Cross-layer awareness is critical in this paradigm, as it allows for a comprehensive understanding of the system's state across both its physical and cyber dimensions, enabling more effective and adaptive defense strategies. Strategic guidance, in this context, involves making informed decisions about when and how to alter hardware configurations and deploy redundancy to best protect the system. This multi-faceted strategy enhances the resilience of CPS against sophisticated cyber-attacks, ensuring their reliability and safety in critical applications.

  4. Title: Development of Quantum Information Theory-based Solutions for Counter UAS PI: Vsevolod Ivanov Lead Institution: Virginia Tech Co-PIs & Institution: none Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $10,000 Summary: The PI seeks support to accelerate the growth of relationships between Corvus Labs and the Virginia Tech National Security Institute with the goal of developing a research and funding portfolio in the area of Quantum Sensing, a destination area investment for NSI. Corvus Labs is based in Blacksburg Virginia, and is a sensor fusion technology company focused on developing autonomous systems for defense and industrial use. These systems are underpinned by a strong portfolio of artificial intelligence models for real-time detection and tracking of aerial, maritime, and ground-based objects, and a physics-first approach to synthetic data generation for rapid and robust model training.

5. Title: Federated Edge Intelligence with Multi-modal Learning PI: Bo Ji Lead Institution: Virginia Tech Co-PIs & Institution: Jin Yi Yoon (VT) Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $10,000 Summary: Edge intelligence relies heavily on the sheer volume of data, which often presents two primary challenges: 1) multi-modal data and 2) the need to process such data near the users. To that end, this project is focused on achieving edge intelligence with multi-modal learning. We will employ federated learning to overcome resource constraints and limited data availability at the individual user level, integrating diverse knowledge across users to enhance the performance of edge artificial intelligence (AI) systems, while preserving data privacy.

6. Title: Enabling On-Device Live Captioning in Mixed Reality Systems PI: Bo Ji Lead Institution: Virginia Tech Co-PIs & Institution: Siwei Cao (VT) Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $10,000 Summary: In recent years, Mixed Reality (MR) technologies have surged in popularity, blending the physical world with digital elements to create environments where physical and virtual objects coexist, enabling real-time interaction [1]. However, there's significant room for improving the MR ecosystem, particularly in enhancing user experience and accessibility features. Live captioning, a highly desired feature not yet implemented, offers real-time transcription of spoken content, greatly enhancing communication accessibility for hearing-impaired users, linguistic learning support for non-native speakers, and comprehension for users irrespective of language proficiency or hearing ability.

7. Title: Post-Quantum Mercurial Signatures PI: Jason LeGrow Lead Institution: Virginia Tech Co-PIs & Institution: None Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $5,000 Summary: In this project we will consider post-quantum mercurial signatures. These schemes are used for anonymous credentials—protocols that allow for fine-grained disclosure of information that enable users to demonstrate that they satisfy some predicate without revealing more information than is necessary. We are investigating existing mercurial signature constructions built from (non-post-quantum) Diffie-Hellman, develop appropriate generalization of the security model, and attempt to develop a post-quantum protocol.

8. Title: OSINT and Generative AI for Cyber Vulnerability Assessment PI: Kurt Luther Lead Institution: Virginia Tech Co-PIs & Institution: none Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $9,205 Summary: Many small businesses are unaware of the cyber risks they face or how to mitigate them. To address this issue, starting in Fall 2023, the PI recruited and trained a team of students to conduct free cyber vulnerability assessments for Virginia small businesses. Vulnerability assessments can have many components, including internal network discovery and vulnerability scanning with tools like Nmap and Nessus; security controls interviews based on frameworks like CIS and LESS; and physical security reviews looking for access control, fire suppression, and water detection. Our team's focus is Open Source Intelligence (OSINT), a form of digital investigation using only publicly available data. OSINT techniques are widely used for many types of investigations in domains ranging from cybersecurity (e.g., reconnaissance for pentesting, cyber threat intelligence) to journalism to human rights. For vulnerability assessments specifically, OSINT uses include attack surface mapping (identifying all publicly-accessible digital assets such as website, servers, webcams, and social media accounts, as well as their vulnerabilities); brand monitoring (examining review sites, social media, and forum posts for mentions of the businesses, including negative rumors and disinformation campaigns); and breach data discovery (finding leaked credentials on the Dark Web or other sources).

9. Title: Research and Workforce Development in Quantum Tomography PI: Wayne Scales Lead Institution: Virginia Tech Co-PIs & Institution: none Funding Program: FY24 Workforce & Industry Engagement FY24 Funds: $9,989 Summary: In general, quantum tomography (QT) involves using measurements of an ensemble of quantum states to reconstruct a quantum state. It is a vital tool in Quantum Information Science and Engineering (QISE) and can be used to analyze or validate performance at the quantum gate level or an overall quantum communication channel. Characterization of a quantum communication channel is crucial for secure quantum communication systems. For example, it has been shown that the performance of Quantum Key Distribution (QKD) security protocols can be increased using QT.

10. Title: Approximate Floquet quantum error correcting codes PI: Jamie Sikora Lead Institution: Virginia Tech Co-PIs & Institution: none Funding Program: FY24 Workforce & Industry Engagement

FY24 Funds: $9,866 Summary: This project will fund PhD student, Ankith Mohan, to do an internship with Dr. Kishor Bharti, a Senior Scientist at A*STAR research institute in Singapore. During this project, Ankith will study an important problem within the study of quantum error correction (QEC). In particular, he will focus on creating a novel QEC code that uses fewer resources than current codes, is easier to experimentally implement, and is customized for specific noise models. Specifically, he will work towards the development of approximate Floquet quantum codes.

- **Program – FY24 Internships**

  1. Title: FY24 NextUp Solutions Internships Responsible Party: Steve Cooper Organization: NextUp Solutions Funding Program: FY24 Internships FY23 Funds: $36,000 Number of Interns: 6 Summary: Next Up Solutions provided 6 internships working with a local county government. The students performed a variety of cybersecurity tasks including: 1) Assist in conducting vulnerability assessments and penetration testing to identify potential security weaknesses in our systems and networks, 2) Support the implementation and maintenance of security controls, policies, and procedures, 3) Participate in the monitoring and analysis of security events and incidents, including log analysis and threat intelligence research, 4) Assist in the development and execution of security awareness training programs, 5) Collaborate with cross-functional teams to identify and mitigate security risks across different departments and projects.

  2. Title: Privacy Notice for Eye Tracking in Mixed Reality Responsible Party: Brendan David-John Organization: VT - MAOP Funding Program: FY24 Internships FY23 Funds: $19,500 Number of Interns: 3 Summary: Students will explore interfaces that relay information about collected sensor data, e.g. eye tracking sensors, and educate users on their privacy implications in different contexts. Specifically, in the context of virtual/mixed/augmented reality in which the application and the sensor data is not well understood by the general user. Students will design interfaces and conduct a pilot user study of the system to evaluate their interface in terms of change in privacy awareness, interruption to user experience, and user preference.

  3. Title: FY24 Global Center for Automotive Performance (GCAPS) Internship Responsible Party: Frank Della Pia Organization: GCAPS Funding Program: FY24 Internships FY23 Funds: $3,000 Number of Interns: 1 Summary: The overall goal of the project will be to research the security concerns and vulnerabilities of a data acquisition system and sensor array placed within a healthcare environment, including: The vulnerability of the system itself to malicious cyberattacks for the sake of protecting personally identifiable data; The potential for the data acquisition system placed within a simulated healthcare environment to interfere with medical equipment; This will be done by building upon previous high-level research that identified security attacks/vulnerabilities and the solutions/products to mitigate them. The primary deliverable for this project will be a research paper summarizing findings.

  4. Title: 5G security testbed design Responsible Party: Carl Dietrich Organization: VT - MAOP Funding Program: FY24 Internships FY23 Funds: $18,000 Number of Interns: 2 Summary: Work with VT students to design an open-source software 5G security testbed. This testbed will be used to test various threat scenarios to be done onto a simulated 5G protocol stack to reveal and categorize vulnerabilities in the network. This testbed is intended to use adaptations of current available 5G open-source software suites in conjunction with commercial off-the-shelf (COTS) software-defined radios.

  5. Title: LLMs for Cybersecurity Responsible Party: Peng Gao Organization: VT - MAOP Funding Program: FY24 Internships FY23 Funds: $10,500 Number of Interns: 2 Summary: We want to develop the next-generation LLM (large language model) agents for cybersecurity applications, such as vulnerability detection, penetration testing, and exploit generation. Students will participate in high-impact research projects and gain hands-on skills in security and LLMs.

  6. Title: CCI SWVA Interns Responsible Party: Machelle Hall Organization: CCI SWVA Funding Program: FY24 Internships FY23 Funds: $8,702 Number of Interns: 2 Summary: These internships involved learning program/project management and research administration for a statewide initiative. The internships included event management, website maintenance and other administrative tasks for the successful implementation of node wide programs and events.

  7. Title: Hume Center Summer Internship program Responsible Party: Ehren Hill Organization: VT – Hume Center Funding Program: FY24 Internships FY23 Funds: $8,532 Number of Interns: 1

Summary: This internship program is intended to be an immersive experiential learning environment for a select group of students, in observance of our Hume Center mission to cultivate the next generation of national security leaders. Students in this program should not only gain experience in research, but also have access to professional development opportunities, networking, and exposure to various IC agencies and national security contracting companies. There will be some days over the course of the internship, e.g., when the students visit the intel community around Washington, D.C., when they may have other obligations during regular working hours.

8. Title: FY24 Virginia Tech Information Technology Internships Responsible Party: Randy Marchany Organization: VT – IT Funding Program: FY24 Internships FY23 Funds: $10,000 Number of Interns: 3 Summary: Student interns will work under the supervision of ITSO operational team analysts. The interns will work in three areas in the VT Information Technology central area. The areas include Cyber Defense, Security Architecture and Risk Management.

9. Title: Cybersecurity for renewables in the power grid Responsible Party: Ali Mehrizi-Sani Organization: VT - MAOP Funding Program: FY24 Internships FY23 Funds: $1,500 Number of Interns: 1 Summary: As the penetration of renewables into the power grid increases, so do their cybersecurity challenges. Cyberattacks can and did cause widespread outages in the power grid. This project creates a graph-based neural network cyberattack detection methodology and test it on the 5GPG testbed at VT Power and Energy Center.

10. Title: Cybersecurity Competition Capacity Building: CTF (Capture the Flag) Author Interns Responsible Party: David Raymond Organization: VT – Cyber Range Funding Program: FY24 Internships FY23 Funds: $10,200 Number of Interns: 3 Summary: 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. Some introductory challenges introduce basic cybersecurity topics and may take only a few minutes for a student to solve. More difficult challenges might require a player to attack weakness in a modern cryptographic system, and may take several hours and advanced expertise. Our CloudCTF platform allows for tailored competitions composed of challenges created or imported by the person or group hosting the CTF

11. Title: Using hackathons to teach security-by-design Responsible Party: Arianna Schuler-Scott Organization: VT - MAOP Funding Program: FY24 Internships FY23 Funds: $18,000 Number of Interns: 2 Summary: In this project, the student will do a literature review on approaches to education in cybersecurity in academia, industry and government. They will be given access to a dataset and will do some data analysis. The output of this project is likely to be at the level of a poster presentation, professional or academic conference. The faculty advisor will support the student in developing professional skills over the course of this project.

12. Title: Aspects of Quantum Computing and Cryptography Responsible Party: Jamie Sikora Organization: VT - MAOP Funding Program: FY24 Internships FY23 Funds: $27,000 Number of Interns: 3 Summary: Students will engage with Dr. Jamie Sikora and Dr. Wayne Scales and have the chance to learn quantum computing and cryptography from the theoretical side and also to interact with real quantum hardware. Students can work together to learn the basics while also working independently on different projects. If they want (and only if they wish to), they can participate in helping with quantum summer camps to teach other students about quantum computing.

3.2.4 Central Virginia Node

This year CVN supported an Experiential Learning Call for Proposals and internship programs at VCU and UVA. In addition, VCU supported the Cyber4n6 program, 6 REU students and 2 interns with $75,000; UVA supported a cohort of 25 students.

- Integrating Artificial Intelligence (AI) into Programming to Develop the Cybersecurity Workforce: An Experiential Learning Pilot for Educators and Students (Riggs) Lay Summary: Programming is a key element of cybersecurity development. Artificial Intelligence (AI) is creating new paradigms for solving problems with code. To responsibly educate computer scientists who will work with increasingly capable AI companions, it is necessary to further investigate how humans with limited technical abilities perceive and interact with these companions. To this end, the proposed work will: (a) assess trust, confidence, stress, and performance of pairs of novice programmers programming with and without an AI teammate, (b) develop guidelines for allocating tasks among human and AI members of a team to maximize trustworthiness and effectiveness, and (c) introduce students to ways in which employers are experimenting with AI tools like Copilot.

Update: Artificial Intelligence-driven Development Environments (AIDEs) offer developers revolutionary computer programming assistance. There is great potential in incorporating AIDEs into Computer Science education; however, the effects of these tools should be fully examined before doing so. Here, a within-subjects study was conducted to compare the programming performance, workload, emotion, and self-efficacy of seventeen novices coding with and without use of the GitHub Copilot AIDE under time pressure. Results showed that using the AIDE significantly increased programming efficiency and reduced effort and mental workload but did not significantly impact emotion or self-efficacy. However, participants' performance improved with more experience using the AI, and their self-efficacy followed. The results suggest that students who try AIDEs will likely be tempted to use them for time-sensitive work. There is no evidence that providing AIDEs will aid struggling students, but there is a clear need for students to practice with AI to become competent and confident using it. These findings are critical to workforce development to be adept in using new AI tools.

Collaborations/Partnerships: Joseph Shelton, PhD at Virginia State University - Dr. Shelton helped us recruit students at VSU for our study and secure a space to run the study at VSU.

- Experiential Learning Through Securing Distributed Learning Systems for IoT Systems (Luo)

  Lay Summary: The capstone project is to support 3-4 senior undergraduate students to learn through a experiential learning opportunity. The high school student mentorship program is to provide high school student with the research opportunities in the STEM field. Artificial Intelligence (AI) has been considered an influential tool that deeply permeates almost every facet of our daily lives (e.g., education, autonomous driving, power systems, and healthcare) which adopt Internet of Things (IoT) devices to collect data. Due to the emergence of IoT systems, the data have been generated in a distributed manner, thus leading to deploying distributed learning systems. In the meantime, current distributed learning systems are suffering from various security threats, such as backdoor attacks, data poisoning, Byzantine attacks, and Sybil attacks. Therefore, it is crucial to protect AI models against the continually growing spectrum of cyber threats. This situation underscores the urgent need for developing a skilled workforce in the field of AI security. The objective of this project is to provide students with a training opportunity in the research of secure AI methodologies for IoT Systems. Specifically, this project will focus on how to train students in designing secure system protocols against various attacks in distributed learning systems, equipping them with essential skills in AI security to get them ready for their journey into the AI security workforce after graduation. Update: During this report period, we have made progress in the following. First, we are training a Ph.D. student to work on watermarking scheme design to protect the watermark stealing. We focus on employing cryptographic algorithm in the design and address the signing dependency issue occurred in the watermarking process. The research outcome is a conference paper submitted to The Network and Distributed System Security (NDSS) Symposium 2025. Second, we were developing a Capstone project to train undergraduate students. The project title is: Determining Sensor Quality on Image Input. It focuses on camera sensors whose quality can be degraded over the time. The team developed an AI-based method to automatically check the quality, thus avoid manual checking. Third, we also developed a high school student mentorship program to mentor high school students from local high schools. This program supported three high school students working on AI and AI security. In particular, we mentored a high school student Devesh Kumar to win the Second Place Award at 2024 Metro Richmond Science and Engineering Fair. Fourth, we are actively seeking external funding opportunities, and have luckily secured one external project from industry. This project focuses on applying AI in power systems.

- Autonomous Vehicle Experiential Learning Course Modules (Park) Lay Summary: In this project, we propose developing and delivering course modules offering experiential learning opportunities for Piedmont Virginia Community College (PVCC) and the University of Virginia students. The autonomous vehicle course modules will include how to design and implement adaptive cruise control (ACC), cooperative adaptive cruise control (CACC), and CACC with an unconnected vehicle (CACCu), using common software programs such as MATLAB and Python. For students to experience these autonomous control algorithms, we will assemble a driving simulator based on an open-source program, Carla, and use it for experiential learning. One of the modules will be an integration of cybersecurity. This will ensure awareness of cyber risks and their impact on autonomous systems. Two PVCC courses and one UVA course are already identified for experiential learning. Update: Developed two driving simulators (one at UVA and the other at PVCC).

- Cultivating Cybersecurity Skills and Collaboration: Empowering Through Cybersecurity Competition Teams (Sonmez) Lay Summary: The project aims to foster skill development and collaboration in the field of cybersecurity through the formation of competition teams at Virginia Commonwealth University and Longwood University. By leveraging the resources available in the Virginia Cyber Range and incorporating experiential learning components, students will be equipped with hands-on training and practical experiences to enhance their cybersecurity skills. The project also emphasizes collaboration and knowledge sharing between the institutions, creating a network of cybersecurity professionals and promoting cross-institutional cooperation. Through a series of milestones and a clear timeline, the project will culminate in an online capture-the-flag competition and participation in the Commonwealth Cyberfusion event. The proposed budget allows for the engagement of a team of 8 students from each university, ensuring a cost-effective investment in developing a competitive and skilled cybersecurity workforce in the Commonwealth. Overall, this project aims to equip students with in-demand cybersecurity skills, contribute to the competitiveness of the Commonwealth's workforce, and foster a collaborative and skilled cybersecurity community. Update: We organized our first in house cybersecurity CTF, 44 students and 21 teams competed. Collaborations/Partnerships: Sanish Rai, PhD at Longwood University - Coached a cybersecurity competition team at Longwood University.

- Cyber4n6 Cyber4n6 is an industry-focused experiential learning program in digital forensics in direct partnership with the Computer Evidence Recovery Section (CERS) at Virginia State Police. The program runs throughout the academic year and offers two tracks: forensic investigator or forensic tool developer. During the AY24-25, CVN will be supporting 5 students throughout this program as they learn through hands-on experience, using real data and tools the CERS uses to solve active cases. The VA State Police are still conducting background checks for their top choices. If all goes well this year, we hope to expand this program throughout the state next year.

- REUs Supported At VCU, 6 students were supported in pursuit of REUs. Over ten weeks, these students honed their research skills in the labs of three researchers who currently are, or previously were, funded through CCI/CVN.

VCU Commonwealth Cyber Initiative Internships – Summer '24 Two students were supported to intern at a start-up in central Virginia, CompassAI. CompassAI works to make non-profits more effective and efficient by crafting custom AI systems. Our students, Hrishita Sehrawath and Anika Makarla, were part of the team working on a project entitled "Agent-Based Modeling of Ethical AI Alignment: Simulating Good and Bad AI Interactions for Robust Content Moderation, AI Safety and Security" during their time with CompassAI. Through this work they increased their technical and professional skills in Cybersecurity, AI, and Computer Science. In the first half of the program the students learned: Soft Skills - Communication, Teamwork, Project Management, and Time Management Technical and Professional Cybersecurity Training: Covered Cybersecurity and Computer Science skills necessary for the field, including Python, SQL, SysAdmin, Networking, and Monitoring System and Network Logs. Completed 8 Google Professional Cybersecurity certification courses through Coursera, qualifying them for entry-level positions in cybersecurity. Certificates can be viewed on their LinkedIn profiles. In the second half of the program, students focused on: Agile and Iterative Development Project: Additional Training - Prepared for a Cybersecurity/AI Safety R&D project, learning additional technical skills (Flowise, OpenAI API, LangChain, Python). Project: "Agent-Based Modeling of Ethical AI Alignment - Simulating Good and Bad AI Interactions for Robust

Content Moderation, Safety and Security”; Working Prototype: Develop and deliver a working prototype by the end of the summer.

UVA Commonwealth Cyber Initiative Internships – Spring ‘24 and Summer ‘24 During January term, an in-person cohort of 25 UVA students participated in an experiential workforce development opportunity which included a training course and two events to help broaden their network and deepen their understanding of the relationship between cloud computing and cybersecurity. Students visited Booz Allen Hamilton Helix Center for Innovation, where they learned about the latest cybersecurity and cloud efforts and networked with employees working in cybersecurity. During this event, students participated in a threat assessment activity to think about security in both a preventative as well as adversarial role. During the second event, students were given the opportunity to network with Amazon and AWS employees who had graduated from UVA.

Chapter 4

CCI Innovation

This chapter summarizes the main achievements in FY24 for the CCI innovation mission line, in particular results of innovation and commercialization programming.

4.1 Hub-led Programs

4.1.1 The CCI MeetUp to StartUp Program

In FY24 the CCI Hub continued a series of meetups across the state to bring together innovation-minded students and local members of the entrepreneurial ecosystem. These informal gatherings are an opportunity for students who are interested in becoming entrepreneurs or commercializing their research to meet with those in the local community who can guide them on their journey. Likewise, these gatherings are an opportunity for local funders to learn about the state of research in universities in their community. The hub hosted meetups in all four regional nodes where six different Virginia-based venture capitalist companies were represented:

- Venture Central
- UVA LVG Seed Fund & New Ventures
- 434
- ICAP
- 757 Accelerate

In FY25 meetups will be scheduled to coincide with the Nodes' student research showcases and a new partnership featuring DC Startup Week.

4.1.2 Cyber Circle Innovation

The CCI Hub team has worked with Circle Innovation out of Vancouver, Canada to design a new program called Cyber Circle Innovation. This program is designed to partner existing Virginia-based small Cyber businesses with Cyber subject matter experts from Virginia universities to fill a gap that will speed up the product to market timeline. For example, if a small company needs product testing and evaluation, CCI will help them find a faculty member with the necessary expertise. Based on agreed upon terms, the company will pay thirty percent of the faculty member's time, while CCI will pay the remaining seventy percent. This program is in its pilot phase and we are actively seeking interested companies in Virginia to work with us.

4.1.3 Tech Transfer Support Fund

In FY24 the CCI Hub initiated a new program called the Tech Transfer Support Fund. CCI is offering technology transfer support funding to faculty at primarily undergraduate institutions to facilitate research commercialization efforts. Eligible faculty may apply for grants up to $8,000 to support patent application fees, legal fees, or other professional support. Faculty must enroll in Innovation Commercialization Assistance Program (ICAP) upon grant approval to continue their commercialization efforts.

4.2 Node-led Programs

In addition to the CCI network-wide programs the Hub administered, the CCI Hub again partnered with the NoVA Node to fund our CATAPULT translational research program, further described below. The four CCI Nodes also funded several innovation programs. Spending in FY24 on innovation programs by the four Nodes was $807,000 and its breakdown by Node is depicted in Figure 4.1.

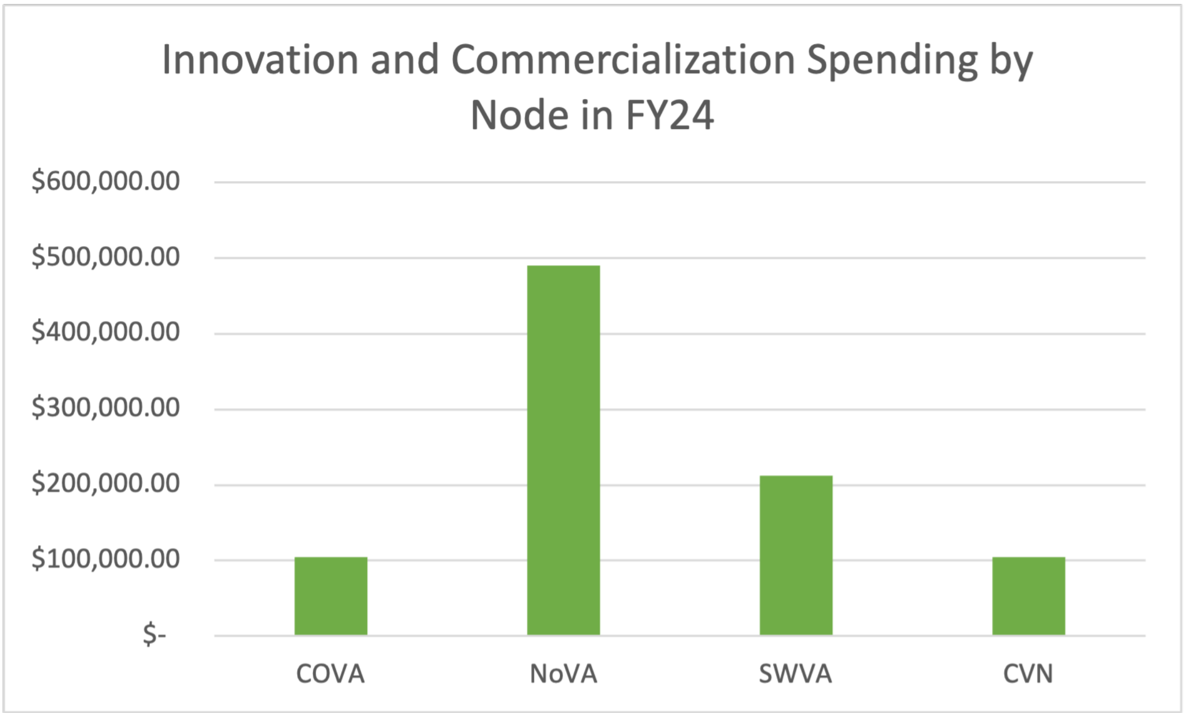


Figure 4.1: Innovation spending by node in FY24.

4.2.1 Northern Virginia Node

In FY24, CCI NoVa Node made investments to expand the number of new cybersecurity solutions in the commercial market by supporting faculty and early-stage companies with wrap around services to promote the successful development of nascent technologies. In FY24, CCI NoVa Node expanded its investment in the highly successful Innovation Commercialization Assistance Program (ICAP) and also continued support for the cybersecurity accelerator based out of George Mason University's Mason Square Arlington Campus, in the heart of the budding Rosslyn-Ballston Tech Corridor.

- **Innovation Commercialization Assistance Program.** ICAP provides long-term mentorship and advising to early-stage, Virginia-based technology companies, and has assisted more than 1200 companies since the program's inception in January 2018. Cybersecurity-related ventures are one of the main focus areas of the program, with roughly 15% of all companies over the past five and a half years having been cyber-focused. In FY24, ICAP, in partnership with George Mason University, began offering access to an NSF I-Corps Lean Startup training program. This program helps participants make the right first steps toward bringing their research to market. Following this course, ICAP Mentors work with clients to provide strategic guidance, connecting them to the right resources at the appropriate time. ICAP Mentors also assist more advanced startups and later-stage cyber companies by preparing them to join accelerator programs, receive investment, and grow their ventures. During FY24, ICAP engaged in 26 companies completing the I- Corps program, including the nine (9) teams from CATAPULT's 2023 cohort. Cybersecurity companies from previous ICAP programs raised $5.19 million in capital and created 13 new jobs in FY24.

- **Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT).** In 2024, CCI continued support for its Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects amongst CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. The CATAPULT Fund is supporting 8 new awards in FY24 of $50,000 each. An investment of $490,000 by CCI NoVa Node was supplemented with $200,000 in funding from CCI Hub. The CATAPULT Fund is an important tool in CCI's Innovation toolbox, providing funding critical to advance the maturity of cyber discoveries during the critical "Valley of Death" phase of commercialization, as defined by the National Science Foundation. During this phase, innovators are preparing for SBIR or CRCF grants to assist in product development and market testing, but are not quite prepared for outside investment. The CATAPULT Fund is helping innovation teams pay for critical resources, personnel, time to test products, and get market initial market feedback integral to obtaining Seed or Angel funding.

  The following 8 projects were funded in FY23:

  - *CATAPULTING Risk Management Framework* (RMF) Compliance through Automation, Artificial Intelligence (AI), and Large Language Models (LLM) George Mason University, EngineeRD Solutions, LLC 05/10/24-06/30/25. The Risk Management Framework (RMF) is a set of guidelines developed by the National Institute of Standards and Technology (NIST) for managing information system(s) risk in organizations, a standard adopted by DoD components as "DoD RMF". There are over 70,000 cyber professionals in DoD performing tasks that include processing security controls and developing RMF compliance packages, managing hundreds of pages of written directives, over 1000 controls, and 5200 procedures. As a result, cybersecurity practitioners spend excessive time on DoD RMF review and compliance, resulting in a more reactive rather than proactive approach towards emerging threats. This project seeks to produce a toolset tailored to DoD RMF processes to determine whether or not such a resource might enhance compliance task efficiency and cybersecurity capabilities.
  - *Real-time Anomaly Detection with Edge AI HaRdware (RADAR)* Virginia Commonwealth University 05/10/24-06/30/25. There is a pressing market need for real-time anomaly detection on edge devices, with limited resources. Current solutions often struggle to be effective in edge computing environments, falling short in accuracy, resource efficiency, and real-time processing. The project team's existing research leads the way in real-time anomaly detection on edge devices with limited resources, leveraging unique autoencoder designs to overcome severe hardware constraints in edge devices. This project will develop a proof-of-concept Field Programmable Gate Array (FPGA)-based in-memory computing system for real-time anomaly detection with unparalleled efficiency and accuracy, adding significant value to the technology by demonstrating its feasibility and effectiveness in real-world edge computing scenarios.
  - *Trustworthy and Explainable AI Framework for Cyber Vulnerability Detection, Risk Explanation, and Defense in Networked CPS: Intellectual Property and Commercialization* Old Dominion University 05/10/24-06/30/25. An increasing amount of networked connected devices and systems become vulnerable due to the limited capability of threat detection and lack of risk severity quantification for defense against them. Apart from conventional computing systems and cloud services, contemporary Internet of Things (IoT), and cyber-physical systems (CPS) face a multitude, and increasing incidence, of cyber threats, presenting a greater challenge to mitigation

efforts. This project develops a trustworthy and explainable artificial intelligence (AI) framework to drive significant improvement in cyber vulnerability detection and risk explanation, as predictive analysis, reasoning, and confidence scores are essential components of the defense against such attacks.

  - *Privacy Guard Accelerator: Next-Generation Privacy Preservation in Deep Learning with Optimized Performance Solutions* Old Dominion University 05/10/24-06/30/25. The integration of Deep Learning (DL) technologies such as ChatGPT, Sora, and MidJourney into a wide array of applications has demonstrated transformative potential across numerous industries, including healthcare, manufacturing, agriculture, and military operations. However, while advanced DL models offer unprecedented capabilities in a number of areas, they also raise significant privacy concerns, especially in interactions with sensitive data. While Fully Homomorphic Encryption (FHE) has emerged as a promising solution to these problems, its prohibitive computational costs make it unfeasible for real- world applications. This project seeks to establish novel strategies and tools to significantly increase FHE's efficiency, broadening the feasibility of privacy-preserved DL for practical applications.
  - *CLAWS: Continuous and Lightweight Authentication for Wearable and Portable Embedded Systems* George Mason University 05/10/24-06/30/25. In the era of digital and smart systems, the number of personal devices per US household is higher than it's ever been, with this number continuing to grow. Along with the number of devices, the number of cyber attacks on these devices has grown exponentially, with lightweight Internet of Things devices often considered the primary target given their multiple constraints. Authentication of these devices is seen as on of the primary and pivotal steps to combat cyber threats. This project develops a new authentication technique, continuously collecting the gait signal of the user and leveraging this unique signal for continuous authentication.
  - *Privacy-preserving Synthetic Data Generation* University of Virginia 05/10/24-06/30/25. Private data synthesis is a process that aims at generating artificial data that preserves both the statistical properties and the structure of real data, while simultaneously protecting privacy. Private data synthesis could have significant implications in a number sectors, from healthcare to finance and beyond. However, meeting the standards listed above has been incredibly difficult. This project seeks to leverage a different standard of privacy guarantee to generate synthetic datasets. The safeguards provided by this standard all but eliminate the existing potential for data leakage, allowing for the broader adoption of this practice by industry.
  - *CyberseQurity: An Automated Tool to Preserve Data and Model Security in Quantum Machine Learning System* George Mason University 05/10/24-06/30/25. Quantum machine learning (QML) is an interdisciplinary field that merges concepts from quantum computing and machine learning, and possesses the ability to dramatically transform a wide range of sectors. However, today's quantum computing relies mostly on cloud computing, following a Quantum-as-a-Service (QaaS) paradigm, presenting the risks of data and model theft during execution that go with it. Current QaaS solutions lack comprehensive mechanisms to safeguard both aspects at run-time, leaving systems vulnerable to attack. This project will develop a resource that offers a unified solution, performing both encryption and optimization at deployment phase, meeting the growing demand for secure quantum computing systems in industries such as healthcare, finance, and defense, while maintaining QML with high performance.

- **CCI+A**. The CATAPULT grants will also trigger recipients' participation in the Commonwealth Cyber Incubator + Accelerator (CCI+A) – launched in early 2022 in the new Digital Innovation Pilot facility on George Mason University's Mason Square campus. CCI+A offers: (1) a bootcamp-style program to rapidly move new technologies forward; (2) support for customer discovery efforts; (3) opportunities for cyber startups to engage with potential industry and government partners, as well as broader DMV- and Commonwealth-based customers; (4) opportunities for customer engagement; (5) opportunities to bring university innovation to industry and government for feedback and collaboration; (6) industry and government collaboration opportunities for cyber faculty on technical work and product testing; (7) opportunities for training students for work in cyber startups; (8) engagement with meaningful student projects; (9) cyber-focused hack-a-thons; (10) cybersecurity- focused workshops, meetings, and collider events with government agencies and industry; and (11) opportunities to engage with seed and venture capital, including the opportunity for exposure to investors and for potential prize money at Mason's annual Accelerate innovation competition. The call for proposals for the CATAPULT fund was released in January 2024, with proposals due February 16, 2024. Eight new companies and faculty partners were notified of their successful selection for CATAPULT funding in April 2024.

In FY 24, seven (7) new patents were granted and eight (8) are pending as a result of CCI NoVa Node researcher endeavors:

- Complex User Authentication Factor Integrating a Sequence of Fingerprints and a Personal Identification Number, Emanuela Marasco and Massimiliano Albanese (George Mason University); patent granted
- Prevention of Web Scraping and Copy and Paste of Content by Font Obfuscation, Mingkui Wei, Yao Liu, Zhuo Lu, Junjie Xiong (George Mason University, University of South Florida)
- Federated Graph Neural Network for Fast Anomaly Detection in Controller Area Networks, Hengrun Zhang and Kai Zeng (George Mason University)
- Methods and Systems for System Call Reduction, Kun Sun and Lingguang Lei (George Mason University); patent granted
- Countering Autonomous Vehicle Usage for Ramming Attacks, Duminda Wijesekera, Santos Jha, Cing-Dao Kan, Zoran Duric, and Fernando Camelli (George Mason University)
- Attack Detection and Countermeasures for Autonomous Navigation, Md Tanvir Arafin (Mason) and Kevin Kornegay (Morgan State University)
- Authenticated Name Resolution, Danny McPherson, Joseph Waldron, and Eric Osterweil (Mason), (VeriSign, Inc.); patent granted
- Systems, Devices, and Methods for Polymorphic Domain Name Resolution, Danny McPherson and Eric Osterweil (Mason), (VeriSign, Inc.); patent granted
- Methods and Systems for Domain Name Data Networking, Eric Osterweil (Mason), Craig Murray, Abedelaziz Mohaisen, and Danny McPherson (VeriSign, Inc.); patent granted
- Techniques for Indicating a Degraded State of an Authoritative Name Server, Burton Kaliski, Eric Osterweil (Mason), Duane Wessels, Frank Scalzo, Glen Wiley, and Shuman Huque (VeriSign, Inc.); patent granted
- Strengthening Integrity Assurances for DNS Date, Burton S. Kiliski, Jr. and Eric Osterweil (VeriSign, Inc.)
- Client Controlled Domain Name Service (DNS) Resolution, Eric Osterweil (Mason) and Ashvatth Lakshmanan (VeriSign, Inc.); patent granted
- Hyperspectral Imaging of Biofluids for Biometric Applications, Emanuela Marasco (George Mason University)
- Method and System for Facilitating a Ranking Score Using Attack Volume to Find Optimal Configurations, Massimiliano Albanese (Mason), Ibifubara Iganibo, Marc E. Mosko, Alejandro E. Brito (Palo Alto Research Center, Inc.)
- System and Method for Determining Vulnerability Metrics for Graph-Based Configuration Security, Massimiliano Albanese (Mason) and Marc E. Mosko (Palo Alto Research Center, Inc.)

4.2.2 Coastal Virginia Node

INNOVATE Cyber: CoVA CCI completed another cohort of its Innovate Cyber Challenge in spring 2024 with a total of 43 students from seven universities and colleges. These included Christopher Newport University, George Mason University, Old Dominion University, University of Virginia, UVA-Wise, Virginia State University, and Virginia Tech. This program groups students into teams and each of the teams are assigned a cybersecurity problem/challenge. Over the semester, the teams use design thinking to produce unique solutions for the problem and present their final product during a Showcase event in April 2024. The teams participating in this years cohort are:

- EMMA
- Virtual Vigilance
- Cyber Chunks
- Cyber Spyder
- CyberScape
- Secure Brain
- EncryptX
- Fortify
- OBOL

4.2.3 Southwest Virginia Node

The Southwest Virginia Node funded two programs under the innovation and commercialization mission line, each with unique projects funded within.

- **Program: Ideation to Commercialization**.
  - Title: CryptoQuest: An Interactive Animation Series for Teaching Cryptography, Post-Quantum Cryptography, and Cybersecurity using Augmented Reality PI: Sherif Abdelhamid Lead Institution: Virginia Military Institute Co-PIs & Institution: Blain Patterson (VMI), Sarah Patterson (VMI), Gretchen Matthews (VT), Hiram Lopez (VT) FY24 Funds: $50,000 Summary: The objective is to develop an interactive animation series to teach high school and university students' various cryptography, cybersecurity, and post-quantum cryptography concepts. The series will be designed to create an immersive learning experience that is engaging, fun, and rewarding. The project team will identify specific learning outcomes for each series episode and use student responses to tailor the content to their understanding levels. The project will align with the CCI mission to advance major research thrusts in cybersecurity and serve as a catalyst for Virginia's long-term leadership in cybersecurity.
  - Title: One Step Closer to Ensuring Supply Chain Data Resiliency: Withstanding Cyber Disruption PI: Myra Blanco Lead Institution: Virginia Tech Co-PIs & Institution: Zeb Bowden, Kevin Kefauver, Mike Mollenhauer (VT) FY24 Funds: $50,000 Summary: This project will address gaps by enabling secure data exchange and sharing through a federated and decentralized data platform with a common governance structure. The platform will standardize the data format and provide governance to the data exchange process; as a result, what and how data is shared will be clearly defined. The platform will be available to all stakeholders in the supply chain, including those in the nautical and aerial sectors. The benefits to the supply chain resulting from the information connectivity provided by our platform are expected to include improved inventory control, shorter turnaround times on fulfillment, increased efficiencies of production development cycles, enhanced predictive insights into end users, and overall enhanced logistics capabilities to design, monitor, and adapt delivery plans. Moreover, the data sharing platform will provide real-time visibility in the transport of goods, thereby improving the ability to forecast potential issues and strengthening supply chain resiliency. This platform will present opportunities to small businesses as well as large organizations at different levels of the supply chain. The equity and accessibility of the data exchanged through our platform will serve as an equalizing force to guarantee benefit to the public as well as the industries involved.

- Title: In-Network Information Flow Control for Lightning-Fast Cross-Host Attack Prevention Enabled by Programmable Switches PI: Peng Gao Lead Institution: Virginia Tech Co-PIs & Institution: Bo Ji (VT) FY24 Funds: $50,000 Summary: In this project, we aim to develop a new network defense system that enables end-to-end network visibility across multiple hosts and enforces security decisions in real time to prevent sophisticated cross-host attacks. Our key idea is to develop a new tag-based network information flow control (IFC) mechanism to precisely track and control inter-host and intra-host information flows, through user-defined IFC tags. The critical challenge is to implement this IFC model and enforce it at the network level in an efficient way, without affecting the linespeed processing of high volumes of benign network traffic in modern enterprise networks. To achieve this, we will develop the first in-network realization of the IFC mechanism, by uniquely leveraging the emerging programmable switches [10] and eBPF [11]. The IFC enforcement occurs entirely within the network data plane, which is essential to lightning-fast attack prevention.

- **Program: FY24 Innovation Program**
  - Title: FY24 Cyber Innovation Scholars and Tech Transfer Bootcamp PI: Node Program FY24 Funds: $62,000 Summary: A group of 31 doctoral candidates, master's students, and postdoctoral researchers attended the Cyber Startup Lab where they were introduced to processes involved in commercializing cyber technology. The 2024 Cyber Innovation Scholars hail from departments across Virginia Tech, including agricultural, leadership, and community education; computer science; electrical and computer engineering; and mathematics. The single-day event furthered CCI's mission to cultivate the next generation of the cyber workforce and make Virginia the best place to start a cybersecurity business. Led by Mark Mondry, director of Virginia Tech's LAUNCH and CCI Southwest Virginia's associate director for partnerships and engagement, the workshop combined seven hour-long start-up labs into a half-day marathon, touching on some of the most critical issues to consider before creating a startup.

4.2.4 Central Virginia Node

This year CVN supported two Calls for Proposals to support Innovation and Commercialization: an internal VCU call and an internal UVA call. Overall four projects were supported.

- UVA Projects
  - How to slip your message under strong interference: Signal alignment use case demonstrations. PI: Nikolaos Sidiropoulos, UVA. Grant Award: $27,500. Lay Summary: The PI has recently proposed a very simple and practical method for reusing spectrum / hiding a covert transmission under a potentially powerful transmitter (e.g., analog or digital radio or TV station). The method leverages repetition coding and a multi-antenna receiver to recover the signal of interest in the face of adverse interference, without any side information. The PI has identified several important use cases for this technology, including anti-jam and emergency communication, Wi-Fi in congested areas, and 'slipping' sensitive communications under commercial radio/TV. The objective of this project is to develop successful demonstrations for select use cases, specifically FM radio and WiFi underlay. These demonstrations will better position us to attract funding specifically for commercialization, and to forge committed partnerships with potential customers in government and industry.
  - PPSDG: A Privacy-preserving Synthetic Data Generator. PI: Tianhao Wang, UVA. Grant Award: $27,500. Lay Summary: Private data synthesis is a process that aims at generating artificial data that preserves the statistical properties as well as the structure of real data, while protecting privacy. This critical problem has a broad range of applications in practice, extending from healthcare to finance and beyond. We propose PPSDG: A Privacy-Preserving Synthetic Data Generator that satisfies the formal privacy guarantee called differential privacy (DP) to generate synthetic datasets. Simply speaking, DP safeguards data by precisely quantifying the allowed privacy leakage, and it is the only widely adopted privacy guarantee in academia. To the best of

our knowledge, there is only one company that provides DP solutions to publish specific results like median salary in different regions (not general synthetic data). Our solution is unique in that it provides synthetic data generation with DP. It is based on our previous and ongoing research, which won several awards at NIST competitions. We will start by building an MVP (minimum viable product). Then, we will conduct customer interviews with customers (mostly government agencies or entities) using this MVP, listening to their needs and walking them through our prototype, using their example data or our prepared public data. In the future, we envision working with different entities to provide support to enable synthetic data generation and/or publication, and we will support ourselves by working with different customers and providing solutions with different extensions (e.g., handling fairness constraints).

- VCU Projects: Two projects will be funded with FY24 funds. The Call for Proposals has closed but the awards have not been decided.

Chapter 5

Collaborative Partnerships and Projects

5.1 Partnerships

5.1.1 CACI

CACI is the inaugural member of the Friends of CCI program. This program is a formal recognition of our partnership that has led to several programs and engagements. CACI is hosting the pilot cohort of our Project-Based Learning Program (section 3.1.3) in partnership with NVCC for the Fall23 and Spring24 semesters. Additionally, CACI has expanded their support of the annual CyberFusion competition for which CCI is a sponsor. CACI has graciously provided speakers for several CCI events such as the VASEM Summit 2022 (section 5.1.3), the CCI Symposium, and the CCI Internship Fair. This year CCI also sponsored CACI's annual CACICon, a company-wide capture the flag competition. In FY24 CACI and CCI have plans to exapand our relationship into research-focused partnerships.

5.1.2 Virginia Economic Development Partnership

In FY24 we have continued to expand our collaboration with Virginia Economic Development Partnership (VEDP), recognizing our common goal of economic development for the commonwealth. This partnership included joint participation in the NSA conference and related events; this is the largest cybersecurity conference and trade show in the world and takes place every spring in San Francisco, CA. The CCI Executive Director and the Innovation and Workforce Development director attended for the second year in a row, partnering with VEDP and VIPC in a reception event for cybersecurity companies interested in doing business in Virginia.

CCI is increasingly requested to make a case to companies and entrepreneurs about the strength of the cybersecurity ecosystem in the commonwealth, including the unique programs we have in workforce development, research, and innovation.

5.1.3 Industry-led Consortia

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 a new 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.

Open Generation Consortium

CCI is also a founding member of the Open Generation Consortium, a privately funded R&D community that brings together diverse technical experts and domain leaders to envision, design, develop, and demonstrate innovative solutions uniquely enabled by emerging 5G capabilities. The consortium is led by MITRE Engenuity, with members from industry, academia, and non-profit organizations.

The current focus of the consortium is in 5G connectivity for drones. CCI, in partnership with MITRE, led the first experiments conducted by the consortium, a proof-of-concept demonstration of 5G connectivity for control of drones, conducted in VT's Drone Park in Blacksburg.

5.2 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 activities in research, workforce development, and commercialization. The next study will be conducted in FY25 and cover fiscal years 2024 and 2025. Economic impact findings and data for FY24 will be included in the CCI FY25 Annual Report.

Below are some economic-related highlights from FY24 that will be included in the FY25 study.

5.2.1 CCI Hub

In FY24, the CCI Hub employed 22 Graduate Research Assistants to conduct cybersecurity research under the direction of Hub research faculty and 3 interns to work exclusively on the CCI xG Testbed under the direction and supervision of the CCI Testbed Director.

CCI also supported and funded 12 students to work on projects for CACI and Microsoft as part of the Project-Based Learning program.

5.2.2 Northern Virginia Node

Seven new patents were granted as a result of CCI NoVa Node research endeavors.

- Complex User Authentication Factor Integrating a Sequence of Fingerprints and a Personal Identification Number, Emanuela Marasco and Massimiliano Albanese (George Mason University). Patent Granted.

- Methods and Systems for System Call Reduction, Kun Sun and Lingguang Lei (George Mason University). Patent Granted.

- Authenticated Name Resolution, Danny McPherson, Joseph Waldron, and Eric Osterweil (George Mason University and VeriSign Inc.). Patent Granted.

- Systems, Devices, and Methods for Polymorphic Domain Name Resolution, Danny McPherson and Eric Osterweil (George Mason University and VeriSign Inc.). Patent Granted.

- Methods and Systems for Domain Name Data Networking, Eric Osterweil, Craig Murray, Abdelaziz Mohaisen, and Danny McPherson (George Mason University and VeriSign Inc.). Patent Granted.

- Techniques for Indicating a Degraded State of an Authoritative Name Server, Burton Kaliski, Erci Osterweil, Duane Wessels, Frank Scalzo, Glen Wiley, and Shuman Huque (George Mason University and VeriSign Inc.). Patent Granted.
- Client Controlled Domain Name Service (DNS) Resolution, Eric Osterweil and Ashvatth Lakssmanan (George Mason University and VeriSign Inc.). Patent Granted.

5.2.3 Coastal Virginia Node

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. One of our industry partners, MI Technical Solutions, has been actively involved in supporting internships. Over the past five years they supported twelve (12) interns and hired 9 of 12, with two currently working as interns.

Old Dominion University, with support from COVA CCI, conducted an analysis of 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 CYSE 368, Internship Course. After gathering and analyzing the data for the students who completed CYSE 368 since 2019, it was determined that 486 students completed an internship experience. In FY24, CoVa Node supported 79 internships.

Student Workforce Development

Since its inception in 2020, COVA CCI supported 462 students in various programs listed in this report. These students worked as research assistants for research projects and participated in the undergraduate research and Innovate Cyber programs. All students developed and gained valuable workforce skills which they will use in their future careers.

A total of 95 students participated in COVA CCI Programs in Fall 2023 and Spring 2024 (FY24), including Undergraduate Cybersecurity Research, Innovate Cyber Challenge, CyberExL, and the Cybersecurity Internship Clinic.

Graduate Research Program

A total of 112 students from seven institutions participated in this program since Spring 2020, with 30 students completing the program during Fall 2023 and Spring 2024 semesters (FY24).

Research Assistants

123 students from multiple institutions at the Post Doctorate, Graduate, and Undergraduate levels. These students are supporting CCI/COVA CCI research projects/activities across multiple semesters/years.

StartUp Companies

NetTech Warriors. As part of the CCI supported Arts and Design Collaboration program, Dr. Kevin Moberly, ODU, and his team, created a cybersecurity game – NetTech Warriors. This game is designed to be used by educators at the K-12 levels to teach students about cybersecurity through an interactive board game. This game has been tested at multiple conferences and at the Art of Cybersecurity exhibit held in the Taubman Museum of Art, Roanoke, Virginia, November 4-5, 2022. NetTech Warriors is still in the early stages of business development, but they plan to develop this game into a fully marketable prototype which can be turned into a commercialized business.

5.2.4 Southwest Virginia Node

Patents and Disclosures

CCI Southwest provides encouragement and support for researchers to file disclosures and patent applications. FY24 saw three new disclosures and three new patents filed.

Ideation to Commercialization Program

Three new programs were funded through this initiative in FY24, each promising to move research from the lab to products benefiting society:

- In-Network Information Flow Control for Lightning-Fast Cross-Host Attack Prevention Enabled by Programmable Switches
- CryptoQuest: An Interactive Animation Series for Teaching Cryptography, Post-Quantum Cryptography, and Cybersecurity using Augmented Reality
- One Step Closer to Ensuring Supply Chain Data Resiliency: Withstanding Cyber Disruption

Internships

Students engaged in internships via several programs supported by CCI Southwest: IT Internships hosted at partner campuses include:

- Virginia Military Institute's ""(SGDT) Smart-built Gamified environment as an autonomous collaborative cybersecurity Digital-Twin facilitating user-behavior modeling in the presence of attacks". This internship program supported fourteen (14) high school students as interns and involved five undergraduates in Lexington and Blacksburg, VA.
- Virginia Cyber Range: Their program entitled "Cybersecurity Competition Capacity Building: CTF Author Interns" supported three (3) undergraduates by participating in the creation of new and interesting Capture the Flag (CTF) challenges.
- CCI SWVA Interns: The CCI Southwest Virginia office hired, onboarded, trained, and worked with two (2) undergraduate student interns: a events management intern and a project management intern.
- Virginia Tech Information Technology Interns: The Virginia Tech IT Security Office (ITSO) and Lab (ITSL) provides a unique opportunity for four (4) undergraduate and graduate students to gain hands-on experience working with cyber security analysts.
- Virginia Tech's Multicultural Academic Opportunities Program (MAOP) Undergraduate Summer Research Internship: Program provides a 10-week undergraduate research internship with Virginia Tech Research Faculty. Students are matched with Faculty in the areas of research interests. Housing and meal plan provided. Competitive monthly stipend. Program events that create an inclusive family atmosphere including a fun weekend retreat. This program supported the cybersecurity research of six CCI SWVA principal investigators by funding thirteen (13) undergraduates to work in their labs.
- The Workforce program "Approximate Floquet quantum error correcting codes" supported one (1) internship with a Senior Scientist at A*STAR research institute in Singapore studying an important problem within the study of quantum error correction.

Cybersecurity Internships with Virginia companies:

- Global Center for Automotive Performance Simulation Internship Program supported one (1) undergraduate intern to research the security concerns and vulnerabilities of a data acquisition system and sensor array placed within a healthcare environment.

- Next Up Solutions provided six (6) internships working with a local county government. The students performed a variety of cybersecurity tasks including: 1) Assist in conducting vulnerability assessments and penetration testing to identify potential security weaknesses in our systems and networks, 2) Support the implementation and maintenance of security controls, policies, and procedures, 3) Participate in the monitoring and analysis of security events and incidents, including log analysis and threat intelligence research, 4) Assist in the development and execution of security awareness training programs, 5) Collaborate with cross-functional teams to identify and mitigate security risks across different departments and projects.

Chapter 6

Financial Report

6.1 CCI Hub

The budget and expenditures for the CCI Hub in FY24 are in Appendix 3.

CCI continued to focus on its three mission lines of Research, Innovation, and Workforce Development in FY24. In FY24, RTI completed the second Economic Impact Study and the results confirmed that CCI continues to have a positive economic impact on the Commonwealth. Detailed data and information from the Economic Impact Study were included in the CCI FY23 Annual Report. The CCI xG testbed is fully operational and researchers and students from across the state used the testbed for experiments and research. In FY24, CCI focused on scaling up successful workforce development and innovation programs to state-wide participation. These programs continue to show positive results and remain popular.

Operations continue to support the CCI mission and the research and innovation communities across the state. CCI conducted its third CCI Symposium in Richmond, VA and hosted three international delegations, as well as, industry and government partners at the VTRC-A to foster collaboration and continue to expand the cybersecurity ecosystem in Virginia. This year CCI supported the National Telecommunications and Information Administration (NTIA) by hosting two ceremonies at the VTRC-A to officially announce the grant award winners from the CHIPS and Science Act Innovation Fund. And finally, CCI hosted its first International Cybersecurity Workshop in Belgium allowing Virginia researchers to travel and collaborate with their European counterparts.

Communications and marketing continued to play a major role with advertising, promoting, covering and branding several CCI sponsored, co-sponsored or attended events in FY24. CCI continues to utilize social media platforms and expand our social media footprint to promote CCI events, researchers and highlight positive impacts across the state in cybersecurity research, workforce development and innovation. To assist with informing interested collaborators and stakeholders, CCI published a series of informative "one-pagers" that highlight an inform readers on the CCI xG Testbed, the Internship and Job Fair, the Project-Based Learning Program, and an easy-to-read summary of workforce development and innovation programs.

CCI continued to sponsor Experiential Learning programs, entrepreneurial incubators, Cyber Fusion 2024, and Project-Based Learning programs to support continued efforts in the workforce development and innovation mission lines. CCI awarded seven grants in the fifth iteration of the Experiential Learning Program and conducted the fourth Internship and Job Fair. Additionally, CCI partnered with CACI and Microsoft to sponsor 11 students in two Project-Based Learning programs that had students work on "real-world" projects under the mentorship and supervision of industry partners. CCI continued to sponsor Meet Up 2 Start Up events to introduce faculty and students interested in commercializing their research to Virginia venture capitalists. These programs are very popular and received positive feedback from participants and CCI will continue to implement improvements based on constructive feedback received through surveys.

In FY24, the CCI xG Testbed was designated an Open Testing and Integration Center (OTIC), one of 17 approved by the ORAN-Alliance worldwide. CCI's role as an ORAN testing and integration center aligns with our mission to spur innovation, integrate security, and lower barriers to entry into the wireless market.

CCI continued to sponsor cybersecurity research programs that foster opportunities for multi-disciplinary research focused on both the technical, as well as, the human side of cybersecurity, data, and autonomous systems. CCI awarded 10 grants to Virginia researchers in the Supply Chain Cybersecurity program. Additionally, CCI awarded six grants to Virginia research teams in the Inclusion and Accessibility in Cybersecurity program. And finally, CCI funded three more Virginia researchers in the CCI Fellows program. CCI researchers from across the Commonwealth continued to attract external funding by submitting high-quality and collaborative proposals that will produce high impact results and continue to move Virginia to a global leader in cutting-edge cyber innovation and research.

6.2 CCI Nodes

In FY24, the CCI Regional Nodes developed spend plans that supported Node objectives, initiatives, and programs that were aligned with their cybersecurity focus areas and the expertise of their research faculty. The Nodes apportioned their funds into three categories: Operations, Research, and Innovation/Workforce Development. Although the categories are the same and all focused on the cybersecurity field, each Node has the flexibility to plan and execute funds so as to best meet the needs of their region and reinforce the cybersecurity research focus of their region's universities and verticals. In FY24, 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 the region.

6.2.1 Coastal Virginia Node

The budget and expenditures for the CoVA Node in FY24 are in Appendix 3.

The Coastal Virginia Center for Cyber Innovation, as a node of the Commonwealth Cybersecurity Initiative, serves as southeastern Virginia's engine for research, innovation, and commercialization of next-generation cybersecurity technologies particularly in the areas of Cyber Physical Systems Security and Artificial Intelligence in maritime, defense, and transportation industries. The Coastal Virginia Center for Cyber Innovation has made significant strides in its first two+ years of existence. Funds are sought to continue the momentum of the initiative.

Central operations staff include a chief administrative official/project manager (1 FTE), office assistant (.5 FTE), and marketing support (.25 FTE). A director and deputy director oversee all aspects of the efforts. In FY24, funds were used to support the administration of the program, research activities, innovation programming, and workforce development programming. Operations funds were also used to coordinate meetings, travel, and activities that promote community among members of the Coastal Virginia Center for Cyber Innovation. Marketing materials were also developed to help promote the activities and success of the Commonwealth Cyber Initiative's Coastal Virginia Center for Cyber Innovation.

Funds to support research were executed in five areas: (1) continued funding of research scientists, (2) funding to support maritime research, (3) funding to support a conference, (4) enhancements of the Coastal Virginia Shared Academic and Research Environment, and (5) funding to support a cluster higher with George Mason University. The cluster hire funds were used to build an inter-institutional research center leveraging the strengths of ODU and GMU. Regarding continued funding of research scientists, funds were required to provide funding for 7 faculty hired at William and Mary, the Old Dominion University School of Cybersecurity, and the Virginia Modeling, Analysis, and Simulation Center. Funds were also be used to continue the support of an IT Engineer to manage the research projects associated with COVA SHARE.

Funds to support regional innovation and development of the talent pipeline were used to promote experiential learning, support undergraduate research, promote student-led innovation programs, provide experiential learning programming for graduate students, support cybersecurity internships, support commercialization, plan and support a cybersecurity workforce development conference and training, and to scale up the CoVA CCI Regional Student Association to the state-wide Virginia Cybersecurity Students (VCyS) association. The undergraduate research program matches students and faculty from across the node to engage in cybersecurity research programs. The Innovate Cyber Challenge brings together students from across the Commonwealth to identify and propose solutions to cybersecurity challenges. The graduate student experiential learning program assigns graduate students from one of the research institutions as graduate assistants to help instructors in node institutions that do not have graduate assistant help. The cybersecurity internship program will be managed through the VSGC with the focus of placing students from coastal Virginia with cybersecurity businesses. A new initiative, Cyber Clinic, focused on hiring students as interns who worked with local government and small businesses on cybersecurity related issues and problems.

6.2.2 Central Virginia Node

The budget and expenditures for the CVN in FY24 are in Appendix 3.

In FY24, CVN used funds to continue to support successful endeavors. Funding support continued for the testbeds that are available for use by the CCI network and continued to foster successful startups. In addition, CVN expanded the development of regional partnerships and strengthening the internship program. Operations funds supported regional staff, a CVN annual meeting, regional partnerships, and general operating expenses. The testbeds backed by CVN funds are inspiring connections throughout the state and as a result CVN continued to subsidize their development. In addition, CVN continued to fund a node-wide research call that required collaboration as well as supporting research faculty. Regional calls for Experiential Learning and Innovation and Commercialization projects were supported with FY24 funds. Remaining funds were split between VCU and UVA to finance internal calls for Innovation and Commercialization and internships.

6.2.3 Northern Virginia Node

The budget and expenditures for the NoVA Node in FY24 are in Appendix 3.

Since FY23, CCI NoVa Node has made major investments in cybersecurity workforce development, attacking the challenge from every potential entry point and through novel modes of training and partnership. NoVa Node has also made significant investments in the development of the cybersecurity innovation ecosystem through the establishment of the CATAPULT fund and the CCI+A cybersecurity accelerator to support cybersecurity startups with seed funds and wrap-around services to ensure their success and anchoring them in the Commonwealth. The NoVa Node's research investments resulted in a mature R&D effort now in direct support of the innovation ecosystem, and serving as a major attractant of external funding to bolster the Commonwealth's Cybersecurity research enterprise. As a portfolio the Nova Node has specifically developed a sphere of investments that are intertwined. Workforce efforts are in direct support of research and the success of entrepreneurship. Research and development efforts are deliberately and directly embedded in the expansion of the cybersecurity innovation ecosystem. This cohesive framework, and record of impact, enables the CCI NoVa Node to scale its success and impact. CCI Investments in the NoVa Node's operations included support for the fulltime project manager who provides day-to-day oversight of CCI NoVa Node programs and partnerships, and a portion of the CCI NoVa Node Director's time. In FY23, CCI NoVa Node engaged in recruiting faculty to the commonwealth. The NoVa Node Living Innovation Laboratory infrastructure and faculty enterprise has significantly matured and is prepared for expansion. We anticipate that recruitment of new faculty expertise to Virginia, and each of the research universities, will enable expansion of Northern Virginia's success in competing for new, externally sponsored research funding - including Federal dollars. In FY24, CCI NoVa Node earmarked funding to support the continued development of each of the research universities' cybersecurity research infrastructure. Additionally, NoVa Node held one open call for research proposals, focusing on the Node's cybersecurity priority areas of impact: national defense, infrastructure, transportation, electric/power distribution, manufacturing sectors and resilience of cyber systems to human behavior. NoVa Node continued to develop industry and government partners to collaborate and support in material ways, the NoVa Node research portfolio. In FY24, the CCI NoVa Node continued to make significant investments in cybersecurity related experiential learning opportunities for high school students, college/university students, and those seeking to upskill into cybersecurity positions in industry and government. These opportunities enabled students to apply classroom knowledge to real world challenges and bridge the "experience" divide. These investments widened the pipeline of cybersecurity career ready talent. In addition, the NoVa Node continued to support each of its program participants to complete Clearance Readiness Program to expand the number of students across the NoVa Node who are prepared to enter and complete the security clearance process, denoting this preparation with an electronic badge so employers can quickly identify these candidates. Investments were made to upskill non-degree seeking candidates, with special emphasis on career changers and those without prior cybersecurity training in order to widen the pipeline. NoVa Node also scaled its undergraduate internships to prepare our students for work in established or emerging companies working at the leading edge of R&D. CCI NoCa Node also engaged in programming to facilitate the interaction between industry and underrepresented populations in the field. Finally, the NoVa Node invested resources in K-12 teacher training in cybersecurity to bring cybersecurity modules and expertise to teachers and enable them to transfer the knowledge across the spectrum of K-12 age groups and classroom subjects. All NoVa Node programs sought to expand the diversity of the cybersecurity workforce. CCI NoVa Node continued to build and expand the cybersecurity innovation and entrepreneur ecosystem in Northern Virginia and across the Commonwealth. In FY24, NoVa Node invested in Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects among CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. A key part of the success of CATAPULT was the investment in CCI+A, the cybersecurity accelerator launched in FY22 with seed support for 8 new cybersecurity start-ups, and the wrap around services to ensure their successful growth in the Commonwealth. In FY24, CCI+A added, and scaled, an additional cohort of new companies. In both the areas of workforce development and innovation and entrepreneurship, CCI NoVa Node is committed expanding diversity in the field, by actively engaging in both traditional and nontraditional settings to promote opportunities and attract increasingly diverse applicant pools for our many programs.

6.2.4 Southwest Virginia Node

The budget and expenditures for the SWVA Node in FY24 are in Appendix 3.

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

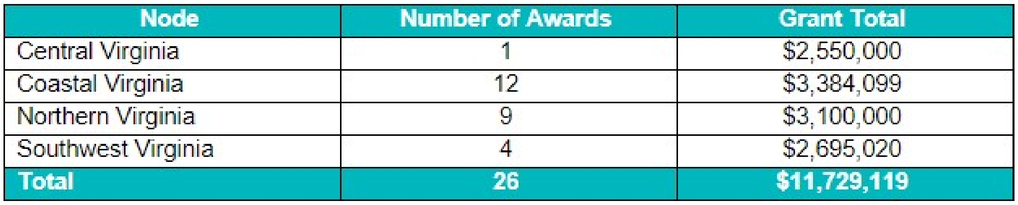
CCI SWVA supported major research initiatives that build on prior investments. Continued funding for some of our major research areas include security of data, communications, power and energy, transportation and cyber-biosecurity resulting in programs in quantum communication, artificial Intelligence assurance, 5G/next-G, wireless security, cryptography, wireless communications and security, system and software security, autonomous vehicle safety, and 5G power grid. Also included was the support of post-doctoral associates and professional development cost for graduate research assistants.

CCI SWVA continued the Regional Innovation thrust by providing funding for three projects in our Innovation call and outreach support of the SWVA innovation community. Talent Pipeline programs included the CCI SWVA Internship Program designed to incorporate all partner institutions and engage SWVA companies and startups. Various workforce programs to engage students at SWVA institutions. SWVA also included funding for a student entrepreneurship program.

6.3 Geographic distribution of the awards from funds contained in HB30

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

Geographic Distribution of Awards from the Funds Contained in HB30



Node	Number of Awards	Grant Total
Central Virginia	1	$2,550,000
Coastal Virginia	12	$3,384,099
Northern Virginia	9	$3,100,000
Southwest Virginia	4	$2,695,020
Total	**26**	**$11,729,119**

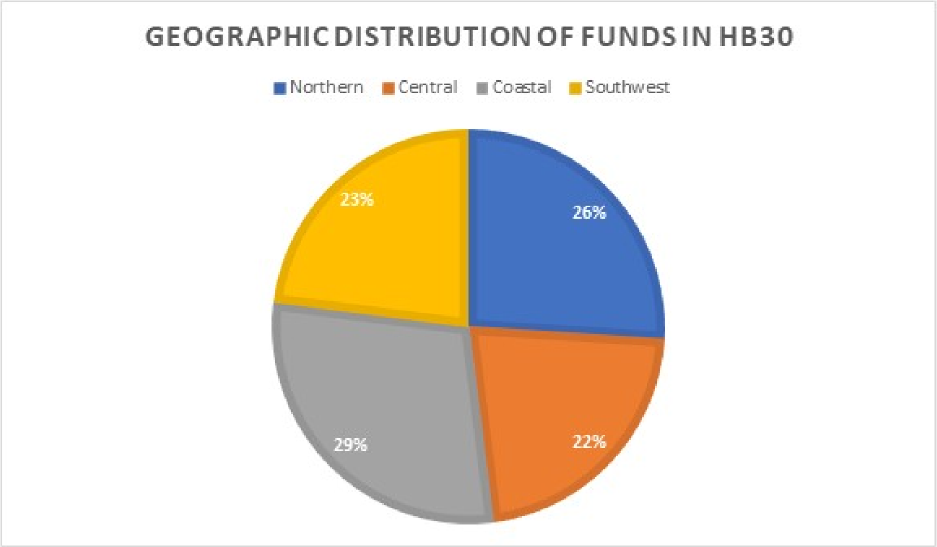


Figure 6.1: Geographic distribution of awards using FY24 funds.

Chapter 7

Looking Ahead: FY25

In FY24 we continued to invest in research, innovation, and workforce development programs launched by the CCI Hub and by each of the regional Nodes. Our biannual economic impact study revealed CCI's most impressive impact on cybersecurity jobs, engagement with companies and the innovation ecosystem, active participation by students throughout the network. Most of this report thus far has been devoted to describing the main accomplishments of the CCI network in FY24. In this chapter, we outline the main activities and programs planned for FY25.

Our major initiatives for the coming fiscal year include:

- Celebration of CCI's fifth-year anniversary.
- Launch of a new industry/university center supported by NSF.
- Investment focus on artificial intelligence for cybersecurity and cybersecurity for artificial intelligence.
- Expansion of our project-based learning program.
- Automation of reporting systems used by faculty and staff supported by CCI programs.
- Establishment of a commonwealth-wide cybersecurity student organization.
- Expansion of international partnerships.
- New and continuing innovation programs.

We discuss each of these goals in turn.

7.1 Celebration of CCI's Fifth-year Anniversary

CCI was established by the Virginia General Assembly in Special Session I in 2018 and has been operational since FY20. This year, we are celebrating our fifth anniversary.

We are taking the opportunity to celebrate the impact that the initiative has had on the commonwealth as well as continue to communicate opportunities for students and companies to engage in our many programs. As part of this celebration we are planning for:

- Developing a visual identity for the fifth anniversary celebration.
- Marking the beginning of the celebration in the CCI Technical Advisory Board (TAB) meeting scheduled for September 2024.
- Highlight the accomplishments of CCI students and faculty during these five years in October 2024, cybersecurity awareness month.
- Closing out the anniversary campaign with a celebration during our annual symposium in Richmond in April 2025.

7.2 Launch of a new industry-university center supported by NSF

A CCI team led by Dr. Luiz DaSilva submited a joint proposal to NSF's Industry-University Cooperative Research Center (IUCRC) program in December 2023. The proposed industry-academia research center, Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks (WISPER), will focus on 6G technology. The team includes researchers from VT, Mason, and the University of Arizona. Our proposal included 24 letters of financial commitment from companies interested in joining the center.

The proposal was selected for funding by NSF, and the new center will launch in August 2024. NSF will provide funding of $450 thousand per year, for five years, for the administration of the center. Each industry member will make a $50 thousand contribution per year for research to be conducted in WISPER. Over its five-year Phase I, WISPER is expected to bring at least $5 million in additional research funding.

This will be the first NSF-funded center bringing together industry and academic researchers on the topic of NextG networks. It will bring global visibility to CCI researchers and strengthen our network of industry partners.

WISPER will coordinate academia, industry, and government to pioneer transformative next generation (NextG) wireless technologies for key industry verticals. Our missions include: (1) growing the U.S. innovation capacity in the next generation wireless networks; (2) catalyzing breakthrough pre-competitive research for enabling NextG wireless communications; (3) contributing to the emerging North American vision for the next generation of wireless networks; (4) providing guidance to standardization bodies and cooperation partners; and (5) producing a workforce prepared to tackle complex next generation wireless challenges.

WISPER will focus on developing transformative wireless innovations. Areas of research include but are not limited to: (1) exploration of new spectrum bands for NextG wireless networks through a holistic lens by considering performance, efficiency, resilience, and security and privacy; (2) deep integration of artificial intelligence in wireless networks; (3) softwarization and virtualization of NextG network functionalities; (4) development of advanced solutions based on quantum and blockchain technologies to support NextG wireless communications; (5) demonstration of NextG wireless networks in diversified industrial applications; and (6) development of an industry-guided workforce development program in the context of next- generation wireless networks.

WISPER will also prepare students to become proficient in NextG techniques, leading to transformative changes in the state of wireless workforce preparedness. WISPER will enable seamless integration of the center's new discoveries into NextG wireless systems, accelerating technology transfer, enhancing the competence of the industrial members, and contributing to the Nation's leadership in NextG technologies.

7.3 Investment focus on artificial intelligence for cybersecurity and cybersecurity for artificial intelligence

Each year, we launch a call for research proposals. These provide seed grants to build capacity on a key topic in cybersecurity and make our researchers more competitive to go after larger-scale funding. In the past, we have funded such calls as 2022's securing human/machine interactions, 2021's securing the next generation of networks, and 2023's supply chain security.

This year, we are looking for proposals that advance AI for cybersecurity and/or cybersecurity for AI. Potential topics include but are not limited to:

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

7.4 Expansion of our project-based learning program

In the pilot year of the Project-Based Learning Program, we worked with CACI to fund seven students for two semesters, to build Capture-the-Flag challenges. We deemed the pilot a success when CACI wanted to work with us for another academic year, and when Microsoft agreed to work with us for two projects. Each project has funded an average of five students, so in order to scale this project, we are working to add more and more companies to our portfolio. By adding more companies to the program, even at an average of five students, we can really make an impact. We believe this program benefits companies, for whom a larger internship programs are unsustainable and for students, to add to their workforce experiences listed on their resumes. The summer 2024 Flipper Zero project at Microsoft was so successful, that several other Microsoft employees have signalled interest in sponsoring new projects. Our current projection is three concurrent projects running at Microsoft.

We are working with area economic development partners such as Arlington and Fairfax EDA, to advertise this program.

7.5 Automation of reporting systems used by faculty and staff supported by CCI programs

The 2022 CCI Economic Impact Study Report by Research Triangle International (RTI), recommended that CCI transition from a paper technical and research reporting system to a digital reporting system. During Fiscal Year 2023, the CCI Hub and Regional Nodes designed, developed and tested a digital reporting system using the America Learns Digital Impact Suite. In Fiscal Year 2024, CCI implemented a pilot program for a limited number of research faculty to complete and submit their technical or annual research reports using the America Learns Suite.

The design goal of the system was to make reporting user-friendly, more efficient, and most importantly, standard across all CCI institutions. Additionally, the system enables data queries to collect, track, and report relevant metrics and demographics, and have data-supported trend analysis and metric tracking. Under this new system, the entire CCI network is answering the same questions and collecting the same information and data. The feedback from the participants in the pilot program was very positive and after implementing some minor changes based on user feedback, CCI is fully implementing the digital reporting system in Fiscal Year 2025.

7.6 Establishment of a commonwealth-wide cybersecurity student organization

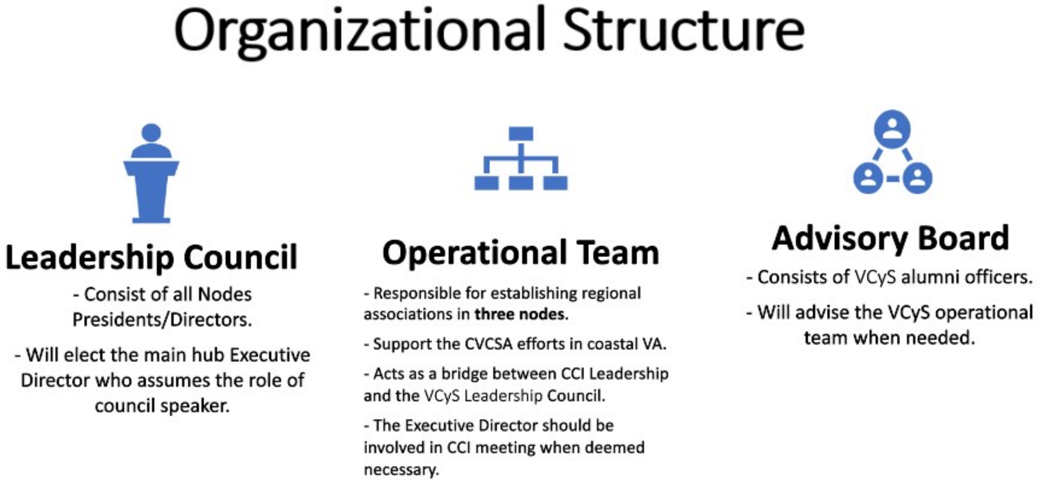
Led by ODU graduate student Zobair Wali and the Coastal Virginia Cybersecurity Student Association (CVCSA), the state-wide Virginia Cybersecurity Student Organization (VCyS) was brought to the CCI Leadership Council to become established to connect and unify the cybersecurity student organizations across the forty-six higher education institutions in the CCI ecosystem. The student organization is structured to match the CCI ecosystem with a hub and four nodes that include a leadership council, operational team, and advisory board to unify, guide, and support Virginia cybersecurity students through collaboration, knowledge, and resource sharing. VCyS' vision is to become the leading force in empowering Virginia's future cyber leaders and professionals. In their inaugural year, FY24, VCyS, in collaboration with the CVCSA member cyber club, organized and hosted a two-day conference and capture the flag event, titled CyberForge, at Christopher Newport University.

The organization's logo and organizational structure are depicted in Figures 7.1 and 7.2, respectively.

7.7 Expansion of international partnerships

Our vision, as stated in Chapter 1, is to establish Virginia as a global leader in cybersecurity. One of the goals for FY25 is to continue to expand our international presence.

Figure 7.1: Virginia Cybersecurity Student Organization Logo.



Organizational Structure

Leadership Council

- Consist of all Nodes Presidents/Directors.

- Will elect the main hub Executive Director who assumes the role of council speaker.

Operational Team

- Responsible for establishing regional associations in **three nodes.**

- Support the CVCSA efforts in coastal VA.

- Acts as a bridge between CCI Leadership and the VCyS Leadership Council.

- The Executive Director should be involved in CCI meeting when deemed necessary.

Advisory Board

- Consists of VCyS alumni officers.

- Will advise the VCyS operational team when needed.

Figure 7.2: Virginia Cybersecurity Student Organizational Structure.

Some specific initiatives include:

- Seek funding for international collaborative research from NSF programs that fund bi-lateral collaborations with other countries.
- Participate in joint initiatives supported by the European Commission towards U.S.-Europe collaborations in advancing cybersecurity.
- Engage with the U.S. Department of State in strategic initiatives on topics such as cybersecurity and O-RAN.
- Build on the success of the first international CCI workshop (Figure 7.3), where we devised a series of actions and recommendations to expand research and innovation partnerships between CCI researchers and some of the top institutions in Europe.
- Engage with key partner nations: in particular, we have joined a transnational cybersecurity organization led by universities in Japan, the U.K., and the U.S.

Figure 7.3: FY24 International Workshop Participants at the Faculty Club of KU Leuven

7.8 New and continuing innovation programs

CCI has recently launched a *MeetUp to Startup* program, where students and faculty with interest in transitioning their research into commercialization can meet with investors and entrepreneurs. These opportunities for informal in-person interactions occur throughout the commonwealth. In FY25, Meetups will coincide with each of the Nodes' student researcher showcases. This will enable participating students to determine if their research has any commercial potential. New in FY25 we plan to capitalize on our membership on the Innovate DMV Steering Committee by hosting a Meetup at DC Startup Week.

The CCI Hub and NoVA Node will continue to co-fund our flagship incubator and accelerator program, CATAPULT. This program, launched in early 2022 and managed by Mason, advances collaborative translational research projects among CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace.

New in FY25 is our Cyber Circle Innovation program, designed in partnership with Circle Innovation out of Vancouver, Canada. This program is designed to partner existing small Cyber businesses with Cyber subject matter experts from Virginia universities to fill a gap that will speed up the product to market timeline. For example, if a small company needs product testing and evaluation, CCI will help them find a faculty member with the necessary expertise. Based on agreed upon terms, the company will pay thirty percent of the faculty member's time, while CCI will pay the remaining seventy percent. This program is in its pilot phase and we are actively seeking interested Virginia companies to work with us.

We also continue to have regular meetings with the VIPC Division of Commercialization to align our innovation programs with opportunities available through the VIPC, such as the Commonwealth Commercialization Fund (CCF), and to make our researchers competitive for such funding.

7.9 CCI 2030: a strategic plan for the next seven years

In FY24, we finalized and released CCI 2030, a strategic plan for the next seven years. The development of the plan was led by the CCI Hub in close partnership with the Leadership Council and the CCI Inclusion and Diversity Committee. The entire CCI network of researchers was asked to provide comments on the first draft of the plan, providing an opportunity for input from a broad array of stakeholders. CCI's TAB provided the final review and recommendations on the strategic plan.

For each of CCI's mission lines of research, innovation, and workforce development, the strategic plan clearly states the role of CCI, our primary goals, programming objectives, tangible outcomes, and indicators of success. The strategic plan articulates our expected impact and will provide important guidance on future investments made by CCI.

The full plan is available on the CCI website. We also had a brochure professionally printed, with highlights of the strategic plan and data on the initiatives' economic impact on the commonwealth (Figure 7.4).

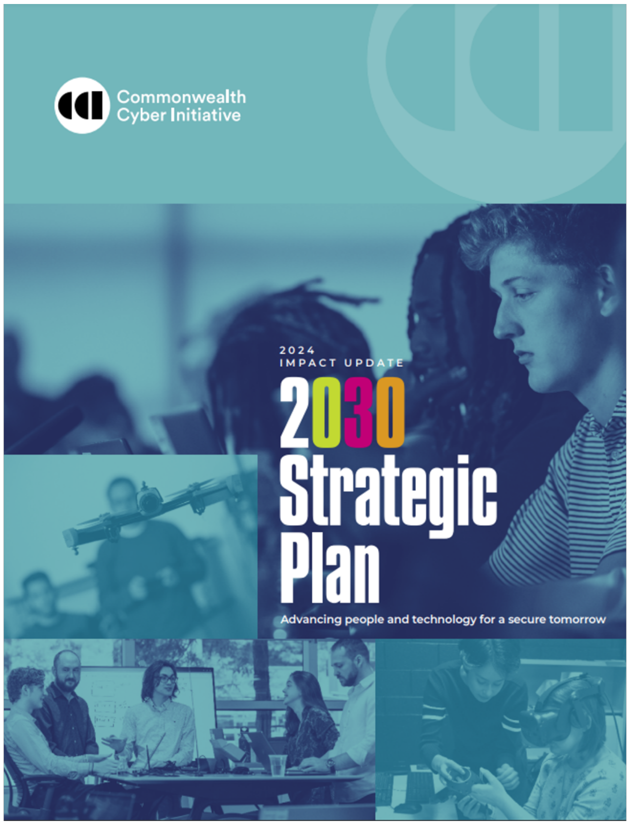

Commonwealth Cyber Initiative
2024
IMPACT UPDATE
2030
Strategic
Plan
Advancing people and technology for a secure tomorrow

Figure 7.4: CCI 2030 Strategic Plan brochure cover page.

Appendices

Appendix 1: CCI Extramural Funding for FY24

Appendix 2: CCI Supply Chain Cybersecurity Research Grants and Inclusion and Accessibility in Cybersecurity Research Grants FY24

Appendix 3: CCI FY24 Financial Reports

Appendix 1: CCI Extramural Funding for FY24

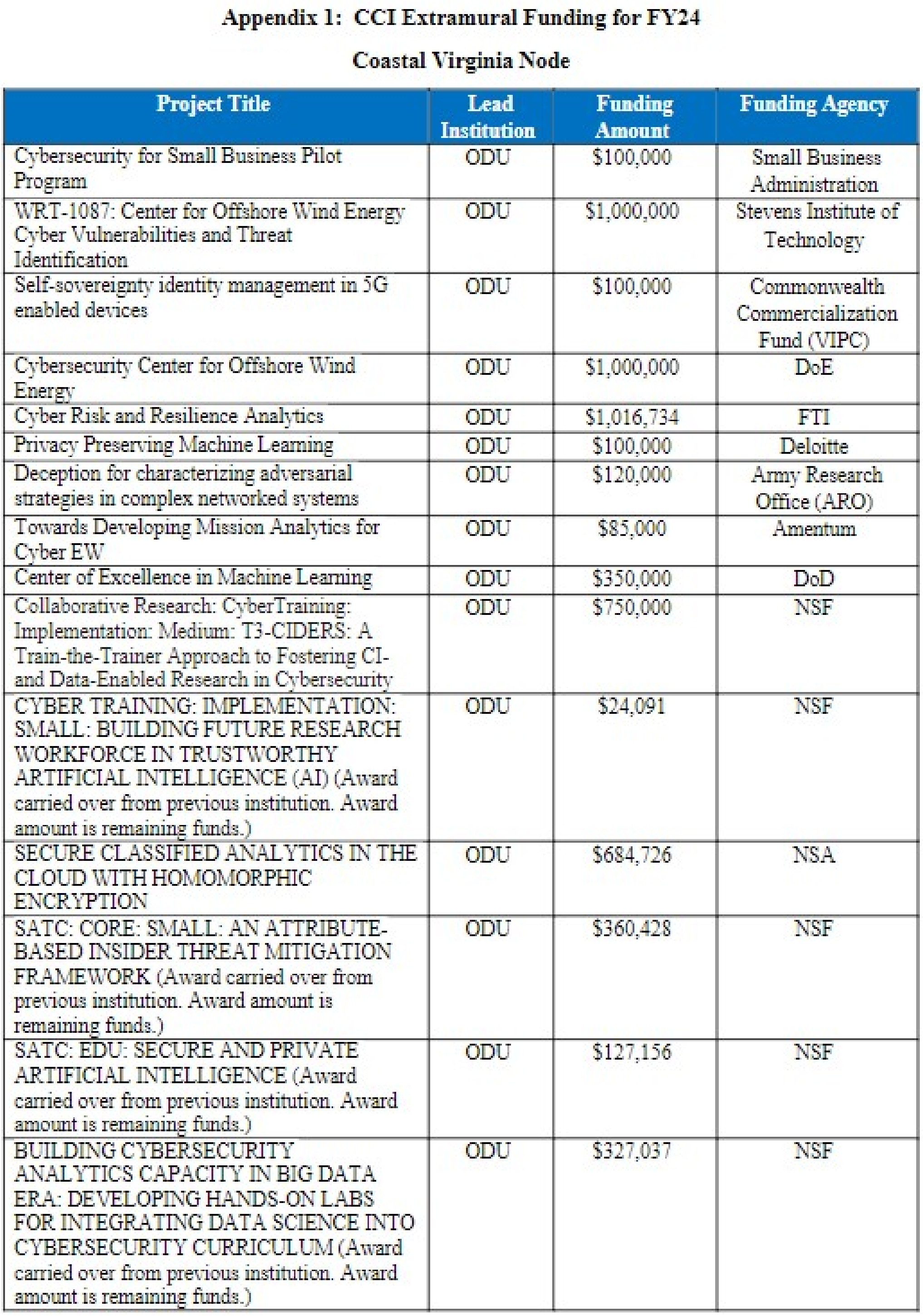
CCI Hub

Project Title	Lead Institution	Funding Amount	Funding Agency
Cyberbiosecurity for air-gapped portable genome sequencing systems	Virginia Tech	$14,451	IARPA & MRI Global
AI-driven farming & supply chain management using causality	Virginia Tech	$100,000	Geminos
SWIFT-SAT: Efficient and On-Demand Spectrum Coexistence for Satellite-Terrestrial Systems	Virginia Tech	$367,498	NSF
EAGER: Toward a Decentralized Cross-Administration Zone Management System: Policy and Technology	Virginia Tech	$150,000	NSF
Establishing Best Practices for Socialization of New Technologies for Effective Integration Post-Acquisition	Virginia Tech	$45,076	Stevens Institute of Technology
Georgetown Cyber SMART IUCRC	Virginia Tech	$24,000	University of Notre Dame
Recovery, Reconstruction, and Mobilization of Ukraine: Cybersecurity and Supply Chain	Virginia Tech	$11,500	Washington Core
Byzantine Resilient Federated Learning in Sporadically Connected Wireless Networks	Virginia Tech	$225,000	ONR
NSF Student Travel Grant for 2024 IEEE International Symposium on Dynamic Spectrum Access Networks (IEEE DySPAN)	Virginia Tech	$15,000	NSF
Acceleration of Compatibility and Commercialization for Open RAN Deployments (ACCoRD)	Virginia Tech	$1,700,000	NTIA
O-Milli-RAN - An O-RAN-compliant, Softwarized mmWave Radio Stack with Flexible PHY and MAC	Virginia Tech	$60,000	NSF
Local 6G Connectivity: Controlled, Resilient, and Secure (6G-ConCoRSe)	Virginia Tech	$599,942	NSF
Collaborative Research: SaTC: CORE: Medium: Securing Next G Millimeter-Wave Communication in Programmable RF Environments with Reconfigurable Intelligent Surfaces (SECURIS)	Virginia Tech	$220,000	NSF
Trustworthy Generative AI for Secure System Operation	Virginia Tech	$75,000	University of Notre Dame
Policy study on Trustable technology for Cyber Physical System	Virginia Tech	$58,000	University of Norte Dame
Total		**$3,665,467**	

Appendix 1: CCI Extramural Funding for FY24

Northern Virginia Node

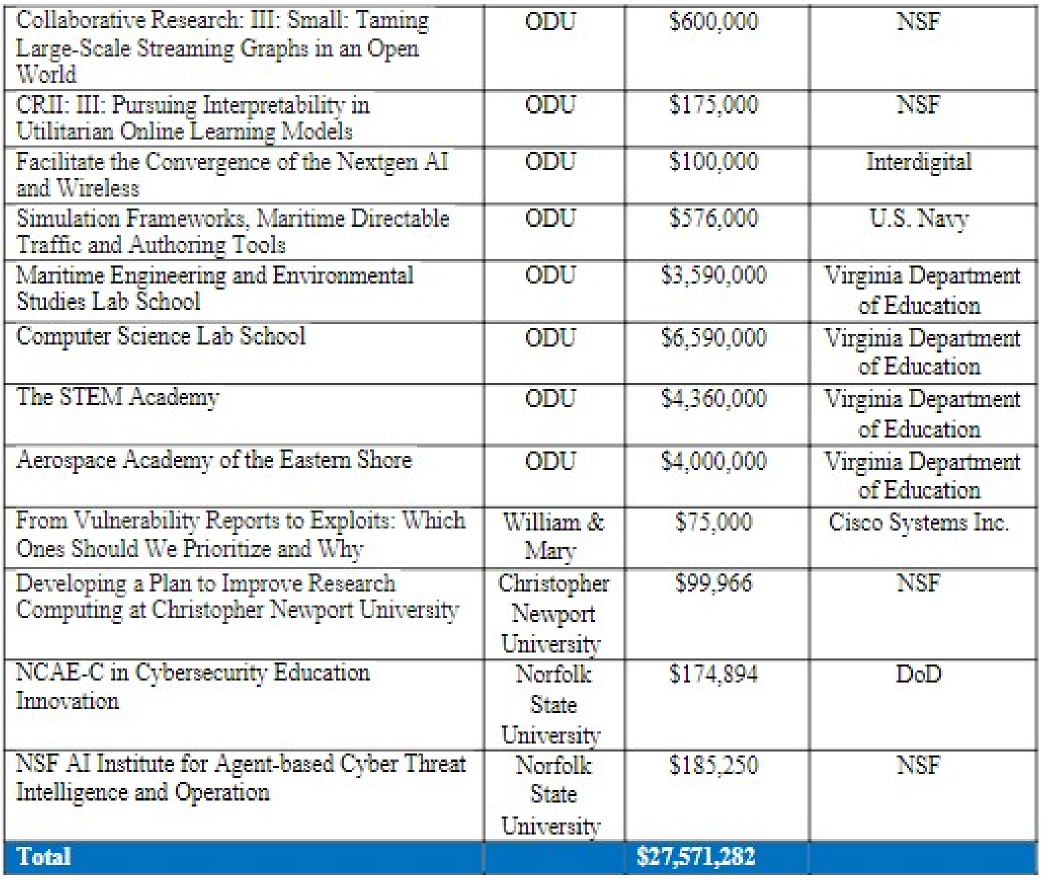
Project Title	Lead Institution	Funding Amount	Funding Agency
Cybersecurity 2023	George Mason	$87,625	NSA
Partnership in NCR	George Mason	$99,999	NSF
ASCEND	George Mason	$145,403	SRI/ARPA
Merlin (Phase 3)	George Mason	$475,791	GMRF/NATO
Metadata Overlay	George Mason	$35,000	Pluribus
Deception Mitigation	George Mason	$170,000	ONR
TAPEE	George Mason	$40,500	CRA
Immersive Computing	George Mason	$99,999	NSF
Jqub	George Mason	$7,000	GMRF
CollabRes: NISQ-era Devices	George Mason	$342,600	NSF
Cyber Training/Quantum Systems	George Mason	$300,000	NSF
EAGER: Inclusive Scam Detection	George Mason	$299,248	NSF
Modeling	George Mason	$243,250	DoD
CollabRes: SaTC: CORE: Med: Infrastructure	George Mason	$120,000	NSF
EAGER: SaTC: Sweaty Digits: Human ID	George Mason	$200,000	NSF
Spectrum Allocation	George Mason	$45,000	SSC/U.S. Navy
CHART2	George Mason	$40,655	STI/USAF
Informed Decision-Making	George Mason	$149,978	USNRC
FW-HTF-RL: Wearable Tech	George Mason	$1,871,692	NSF
Enhancing Cybersecurity Education	George Mason	$199,901	DoC
CoreRes: Tools and Decision Making	George Mason	$41,500	SIT/DoD/AIRC
Photonics (Phase II)	George Mason	$600,000	NCMS/DoD
SAFE SiM	George Mason	$28,044	KadSCI/DARPA
IBODC2 Software	George Mason	$349,997	ARFL
Integration – Large: M2	George Mason	$500,000	NSF/CC
Cybersecurity Testing	George Mason	$476,375	DoC
mmWave 5G	George Mason	$40,000	NSF
CollabRes: Protein Language Model	George Mason	$599,948	NSF
CollabRes: IIBR: Molecule Gen	George Mason	$97,078	NSF
AFCENT	George Mason	$2,413,500	CACI/AFRL
LLMs4Bio	George Mason	$19,494	NSF
Auto Security Patch Generation	George Mason	$470,734	ONR
Friendly Forces ID	George Mason	$5,000	SIT/DoD
Portfolio	George Mason	$23,395,381	DoD/CDAO
Advisory for Ivory Coast	George Mason	$100,000	CIT
Integration	George Mason	$40,000	Syntek/FHWA
CollabRes: SHF: SourceCode	George Mason	$72,703	NSF
Virtual Reality Applications	George Mason	$50,000	NSF/I-Corps
NAACL	George Mason	$20,000	NSF
mmWave Testbed	George Mason	$250,000	U.S. Army
CollabRes:SATC: Core: Med: SECURIS	George Mason	$268,300	NSF
CollabRes: Powered Back Scatter	George Mason	$280,000	NSF
5G Radio Access Networks	George Mason	$700,000	DoC
Enabling Zero Trust Authentication for Metaverse	George Mason	$98,185	Cisco Systems Inc.
Total		**$35,512,447**	



Appendix 1: CCI Extramural Funding for FY24

Coastal Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Cybersecurity for Small Business Pilot Program	ODU	$100,000	Small Business Administration
WRT-1087: Center for Offshore Wind Energy Cyber Vulnerabilities and Threat Identification	ODU	$1,000,000	Stevens Institute of Technology
Self-sovereignty identity management in 5G enabled devices	ODU	$100,000	Commonwealth Commercialization Fund (VIPC)
Cybersecurity Center for Offshore Wind Energy	ODU	$1,000,000	DoE
Cyber Risk and Resilience Analytics	ODU	$1,016,734	FTI
Privacy Preserving Machine Learning	ODU	$100,000	Deloitte
Deception for characterizing adversarial strategies in complex networked systems	ODU	$120,000	Army Research Office (ARO)
Towards Developing Mission Analytics for Cyber EW	ODU	$85,000	Amentum
Center of Excellence in Machine Learning	ODU	$350,000	DoD
Collaborative Research: CyberTraining: Implementation: Medium: T3-CIDERS: A Train-the-Trainer Approach to Fostering CI- and Data-Enabled Research in Cybersecurity	ODU	$750,000	NSF
CYBER TRAINING: IMPLEMENTATION: SMALL: BUILDING FUTURE RESEARCH WORKFORCE IN TRUSTWORTHY ARTIFICIAL INTELLIGENCE (AI) (Award carried over from previous institution. Award amount is remaining funds.)	ODU	$24,091	NSF
SECURE CLASSIFIED ANALYTICS IN THE CLOUD WITH HOMOMORPHIC ENCRYPTION	ODU	$684,726	NSA
SATC: CORE: SMALL: AN ATTRIBUTE-BASED INSIDER THREAT MITIGATION FRAMEWORK (Award carried over from previous institution. Award amount is remaining funds.)	ODU	$360,428	NSF
SATC: EDU: SECURE AND PRIVATE ARTIFICIAL INTELLIGENCE (Award carried over from previous institution. Award amount is remaining funds.)	ODU	$127,156	NSF
BUILDING CYBERSECURITY ANALYTICS CAPACITY IN BIG DATA ERA: DEVELOPING HANDS-ON LABS FOR INTEGRATING DATA SCIENCE INTO CYBERSECURITY CURRICULUM (Award carried over from previous institution. Award amount is remaining funds.)	ODU	$327,037	NSF



Collaborative Research: III: Small: Taming Large-Scale Streaming Graphs in an Open World	ODU	$600,000	NSF
CRII: III: Pursuing Interpretability in Utilitarian Online Learning Models	ODU	$175,000	NSF
Facilitate the Convergence of the Nextgen AI and Wireless	ODU	$100,000	Interdigital
Simulation Frameworks, Maritime Directable Traffic and Authoring Tools	ODU	$576,000	U.S. Navy
Maritime Engineering and Environmental Studies Lab School	ODU	$3,590,000	Virginia Department of Education
Computer Science Lab School	ODU	$6,590,000	Virginia Department of Education
The STEM Academy	ODU	$4,360,000	Virginia Department of Education
Aerospace Academy of the Eastern Shore	ODU	$4,000,000	Virginia Department of Education
From Vulnerability Reports to Exploits: Which Ones Should We Prioritize and Why	William & Mary	$75,000	Cisco Systems Inc.
Developing a Plan to Improve Research Computing at Christopher Newport University	Christopher Newport University	$99,966	NSF
NCAE-C in Cybersecurity Education Innovation	Norfolk State University	$174,894	DoD
NSF AI Institute for Agent-based Cyber Threat Intelligence and Operation	Norfolk State University	$185,250	NSF
Total		**$27,571,282**	

Appendix 1: CCI Extramural Funding for FY24

Central Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Development of a holistic Smart City Index supporting sustainability, resilience, and economic growth/ Abdelwahed		$25,000	Micron
Real-time Anomaly Detection with Edge AI HaRdware (RADAR)/ Atulasimha		$50,000	CCI+A CATAPULT
Hardware AI/ML anomaly detection/image classification in edge device/ Atulasimha		$100,000	DoD Convergence Lab
Computational RFID/ Stan			Northrop Grumman
SCH: INT: Context-Aware Micro-Interventions for Social Anxiety/ Barnes		$1,200,000	NIMH
The Convergence Laboratory Initiative/ Dhar		$9,000,000	U.S. Air Force
Collaborative Research: IMR: MM-18: Automating Privacy-Preserving Data Sharing of Campus Network Traffic Logs / Sun		$549,947	NSF
Virtual Reality Bike Simulator for End-User Behavior Testing / Heydarian		$85,000	Leidos
Total		**$11,169,947**	

Appendix 1: CCI Extramural Funding for FY24

Southwest Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Using Intelligent Conversational Agents to Empower Adolescents to be Resilient Against Cybergrooming	Virginia Tech	$855,127	NSF
CAREER: Securing and Evolving Internet Security Protocols for Naming and Routing	Virginia Tech	$691,258	NSF
SWIFT-SAT: Efficient and On-Demand Spectrum Coexistence for Satellite-Terrestrial Systems	Virginia Tech	$749,999	NSF
Collaborative Research: NeTS: Medium: An Integrated Multi-Time Scale Approach to High-Performance, Intelligent, and Secure O-RAN based NextG	Virginia Tech	$900,000	NSF
CPS: Medium: Collaborative Research: Robust Sensing and Learning for Autonomous Driving Against Perceptual Illusion	Virginia Tech	$500,000	NSF
Durable Safety: Ensuring Safety Alignment in Post-Fine-Tuning LLMs	Virginia Tech	$75,000	Cisco
Gift to VT Power and Energy Center	Virginia Tech	$100,000	American Electric Power Foundation
Learning-Based ORAN Testing	Virginia Tech	$1,400,000	NTIA
Mobile Distributed MIMO: Learning Meets Spreading in Networking	Virginia Tech	$9,020,542	Advanced Technology International
Open Programmable Secure 5G (OPS-5G)	Virginia Tech	$196,753	Perspecta labs Inc.
Developing IT and Cybersecurity Certification Pipeline to Advance Cluster Growth	Virginia Tech	$202,872	GO Virginia
Symmetries and Fundamental Parameters of Linear Error Correcting Codes, Seed funding for Collaboration and Partnership Projects (SCPP) Phase II	Virginia Tech	$12,000	Indian Institute of Technology Bombay Industrial Research and Consultancy Centre
Secure & Trustworthy Data & Technology	Virginia Tech	$30,000	4-VA
CPS: Small: Collaborative: CYDER: CYbersecure Distribution systems with power Electronically interfaced Renewable— Supplement	Virginia Tech	$142,000	NSF
Microgrid Reliability and Resiliency Research	Virginia Tech	$250,000	DoD
"HVDC-Learn: Modules for Education and Workforce Training in High Voltage Direct	Virginia Tech	$98,000	DoE
Raytheon Fellows program	Virginia Tech	$450,000	Raytheon Technologies
IC Centers for Academic Excellence, year 4	Virginia Tech	$200,000	ODNI

ExpandQISE Track 1: The Prairie View A&M University - Virginia Tech University Quantum Science and Engineering (QISE) Partnership	Virginia Tech	$240,000	Prairie View A&M University
Weakly-Supervised Clinical Variable Extraction for Sepsis Research with Large Language Models	Virginia Tech	$25,000	Children's National Hospital
Fact-Checking in Open-Domain Dialogue Generation through Self-Talk	Virginia Tech	$65,000	Amazon
Machine Learning Analysis of Ultrasound Images for the Investigation of Thoracolumbar Myofascial Pain and Therapeutic Efficacy of Hydrodissection	Virginia Tech	$31,231	DoD
Evaluation of Innovative Placenta Imaging Techniques in Fetal Growth Restriction	Virginia Tech	$12,000	Carilion Clinic
Novel Real-Time Speed of Sound Imaging to Assess Liver Fat: Phantom Study Phase	Virginia Tech	$103,735	Siemens Medical Solutions USA, Inc.
Towards Realtime High-resolution Treatment Monitoring in Humans: Using Ultrasound Imaging to Monitor Low-Intensity Focused	Virginia Tech	$129,961	Focused Ultrasound Foundation
"Timing-based Cache Side-Channel Attacks	Virginia Tech	$30,000	4-VA
Cyberbiosecurity for air-gapped portable genome sequencing systems	Virginia Tech	$54,500	IARPA
AI-driven farming & supply chain management using causality	Virginia Tech	$100,000	Geminos
IMR: MT: Tools for Measuring Route Origin Validation in Resource Public Key Infrastructure (RPKI) at Scale	Virginia Tech	$599,997	NSF
Foundations of Scalable and Resilient Distributed Real-Time Decision Making in Open Multi-Agent Systems	Virginia Tech	$475,637	NSF
Foundations of Resilient Distributed Resource Allocation in Open Networks	Virginia Tech	$422,093	AFOSR
Size-Segregated Particle Odor Chromatographic Kernel (SPOCK)	Virginia Tech	$870,087	IARPA
DoD Cyber Scholarships	Virginia Tech	$1,352,358	DoD
III: Medium: Towards Inclusive Recommendation Systems with Stakeholder Alignment	Virginia Tech	$1,159,223	NSF
Safe RL for Interactive Systems with Stakeholder Alignment	Virginia Tech	$87,500	Amazon
Securing Compartmented Information with Smart Radio Systems (SCISRS)	Virginia Tech	$1,408,193	IARPA
Phononic Traveling Wave Parametric Amplification using Heterostructures of Highly Nonlinear Materials	Virginia Tech	$350,000	DARPA
Multi-Agent Training Exercise (MATrEx)	Virginia Tech	$2,500,000	DARPA
Automotive Cybersecurity projects	Virginia Tech	$2,813,608	Portfolio
Accenture Agri Cybersecurity	Virginia Tech	$75,000	Accenture
UPWARDS: US-Japan Network to Strengthen and Expand Collaboration between Universities on Research and Education in Semiconductors	Virginia Tech	$3,470,000	NSF
ACED: ROOTS: Real-time Optimization of Transceiver Systems	Virginia Tech	$500,000	NSF
A Holistic Cybersecurity Testing Framework for 5G Radio Access Networks	Virginia Tech	$2,000,000	NTIA
Next Generation Emergency Networks	Virginia Tech	$166,500	National Institute of Justice
Total		**$34,915,674**	

Appendix 2: Supply Chain Cybersecurity Research Grants

Central Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Decentralized Detection of Software Supply Chain Attacks through Data Provenance Analytics	Wajih Hassan	University of Virginia	$50,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Explainable Artificial Intelligence (XAI) Security for Logistic Disruption Mitigation in Distributed UAV Swarms	Lida Haghnegahdar	Old Dominion	$50,000
Securing the Machine Learning Components of Autonomous Systems: Risk Assessment and Mitigation	Evgenia Smirni	William & Mary	$100,000
Investigating Security and Privacy by Design for Teleoperated Autonomous Vehicles	Sidi Lu	William & Mary	$50,000
Intelligent Zero Trust for Defense Against Generative AI Attacks in Power Grid Supply Chain	Md Shirajum Munir	Old Dominion	$100,000
CPS: A Trusted Decision-Making System for Autonomous Driving in Supply Networks with Untrusted Components	Katherine Smith	Old Dominion	$50,000
Enhancing Security of Software Supply chain - A Focus on AI/ML	Mohammad Ghasemi Gol	Old Dominion	$50,000
Advancing Supply Chain Security through Quantum Computing: A Framework for Rapid Optimization	Qun Li	William & Mary	$50,000
A Paradigm Shift: Innovating Supply Chain Security for AI-Assisted Devices	Rui Ning	Old Dominion	$100,000

Appendix 2: Supply Chain Cybersecurity Research Grants

Northern Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Towards Lifetime Supply Chain Security for Internet of Things: Testing an Update Before Trusting It	Qiang Zeng	George Mason	$50,000
Underpervised Binary Code Translation for Low-Resource Architectures with Applications to Vulnerability	Lannan Lisa Luo	George Mason	$50,000
Cyber Sentinel: Safeguarding Autonomous Vehicle Supply Chains against Backdoors and Hardware	Sai Dinakarrao	George Mason	$100,000
Securing the Supply chain of Large Language Models as Software with Explainable AI and Humans in the Loop	Ziyu Yao	George Mason	$50,000
Fingerprinting Technology for Enhancing 5G? NextG O-RAN Supply Chain Risk Management	Vijay Shah	George Mason	$50,000
Securing Chiplet-based Semiconductor Manufacturing from Untrusted Supply Chains	Md Tanvir Arafin	George Mason	$50,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Grant Amount
RF Emanations Analysis for Supply Chain Microelectronics Risk Evaluation (RESTORE)	Yi Shi	Virginia Tech	$50,000
An Empirical Evaluation of Large Language Models (LLMs) in Generating Security Tests to Mitigate Supply Chain Attacks	Na Meng	Virginia Tech	$50,000
Cybersecurity Threats in a Federated Supply chain Architecture	Zach Bowden	Virginia Tech (VTTI)	$50,000
Securing Large Language Models for Enhanced Supply Chain Cybersecurity	Ming Jin	Virginia Tech	$50,000

Appendix 2: Inclusion and Accessibility in Cybersecurity Research Grants

Coastal Virginia Node

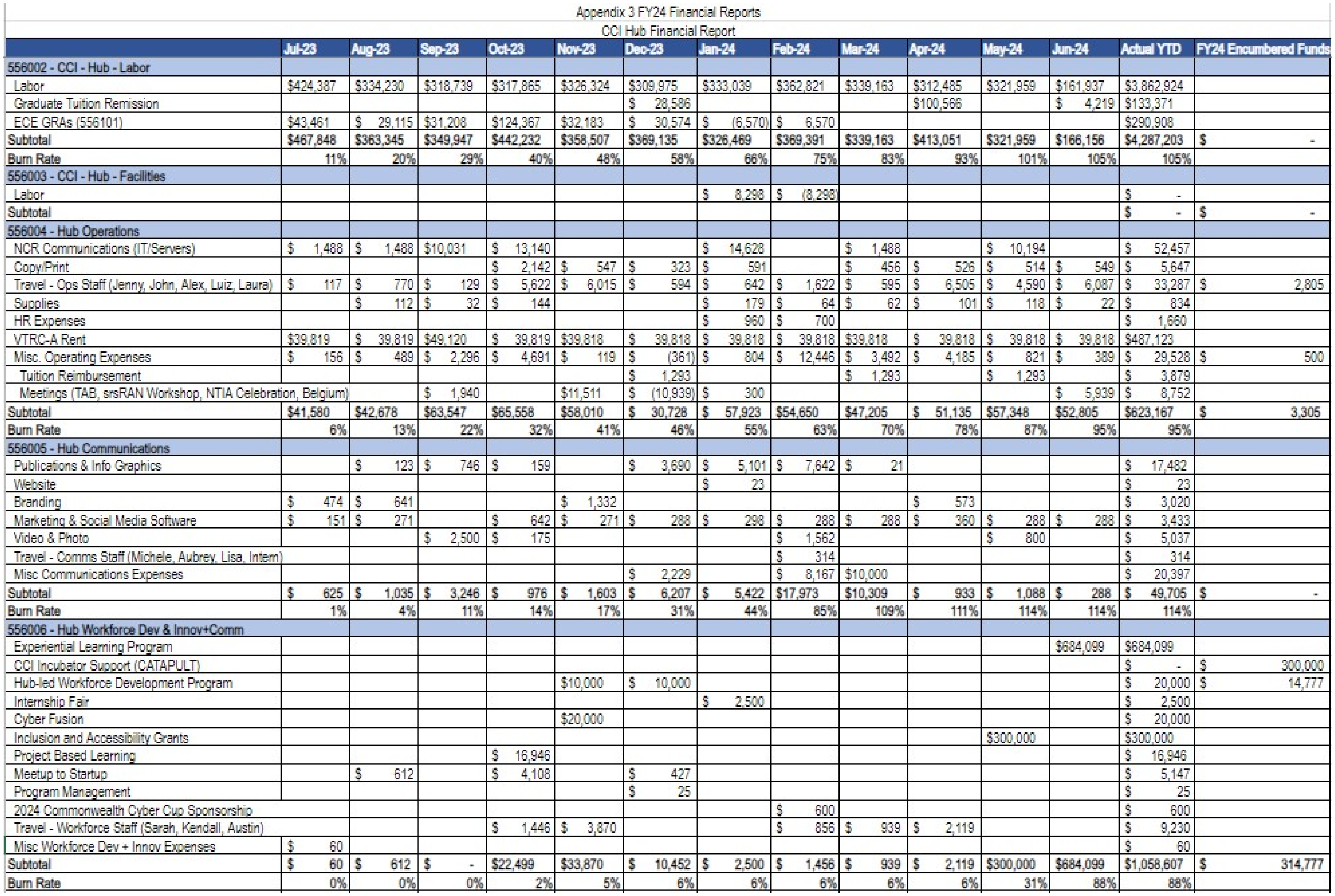
Project Title	PI	Lead Institution	Grant Amount
Bridging the Communication Gap in Cyber Hygiene Material	Mary Still	Old Dominion University	$50,000
Brain-Computer Interface for Password Input: Enhancing Accessibility Individuals with Mobility Impairment	Yanfu Zhang	William & Mary	$50,000
Tackling Dark Pattern-Induced Online Deception of People with Visual Disabilities	Vikas Ashok	Old Dominion	$50,000

Northern Virginia Node

Project Title	PI	Lead Institution	Grant Amount
Data-Centric Social Bias Mitigation for Large Language Model-based	Ziwei Zhou	George Mason	$50,000
Secure and Accurate Implicit Authentication and Continuous Monitoring of Everyday Object Usage for Individuals and Disabilities	Lannan Lisa Luo	George Mason	$50,000
From Data to Defense: Designing Social Cyber Vulnerability Measures to Protect Older Adults Online	Hermant Purohit	George Mason	$50,000
Identity Verification in Smartphones as Social Intersectionality: Inclusive Design of Contactless Fingerprints to Mitigate Skin Tone and Gender Bias	Emanuela Marasco	George Mason	$50,000
Vicarious Offensive Language Verification	Marcos Zampieri	George Mason	$50,000

Southwest Virginia Node

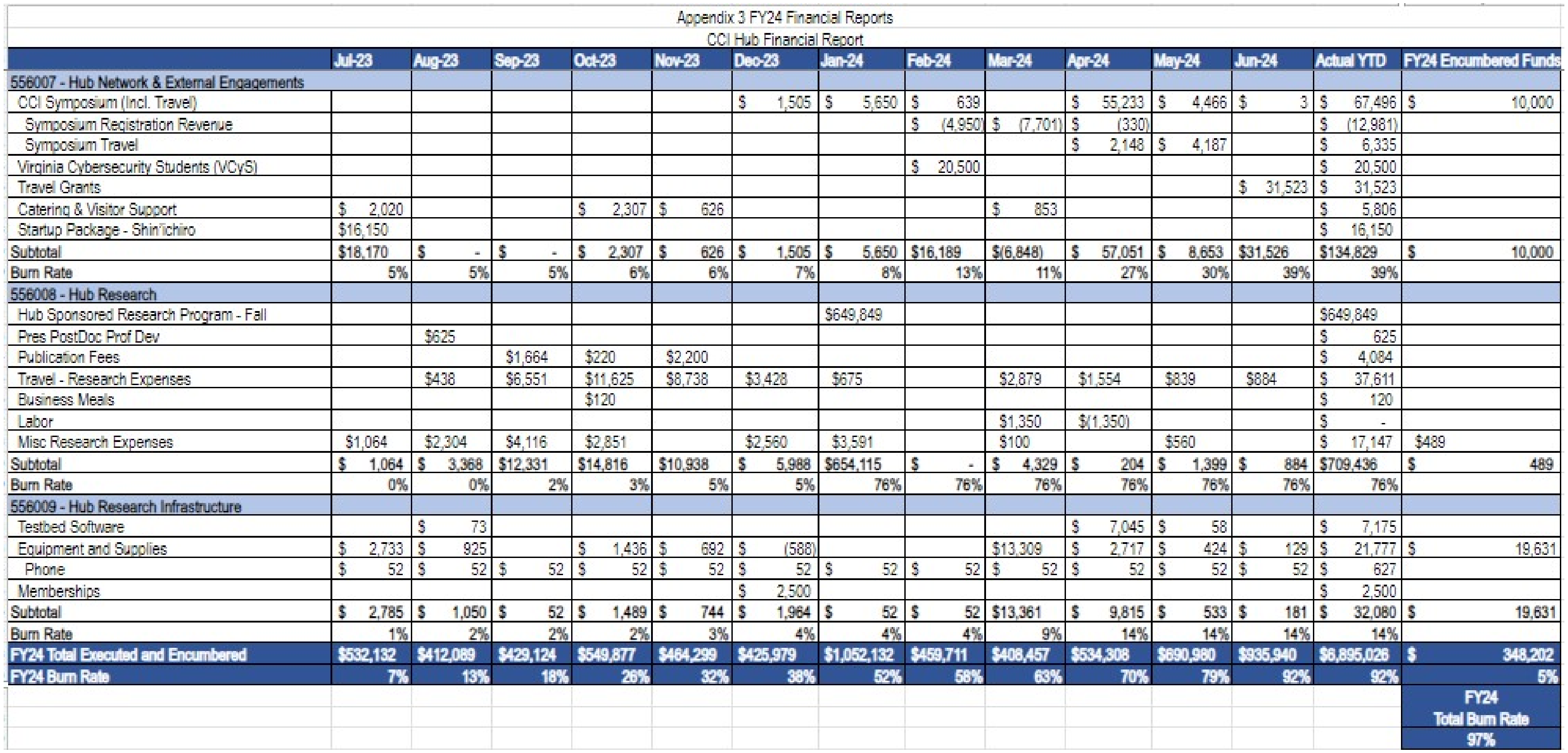
Project Title	PI	Lead Institution	Grant Amount
Enhancing Cybersecurity, Accessibility and Equity Through Inclusive Biometric Authentication	Abhijit Sarkar	Virginia Tech	$50,000
'Don't Dare Judge Me' Judgments by AI Tools and their Impact on Minorities	Tabitha James	Virginia Tech	$50,000
Defending Against Malicious LLM-Driven Agents Utilized for Online Abuse Directed at At-Risk Communities	Bimal Viswanath	Virginia Tech	$50,000



Appendix 3 FY24 Financial Reports

CCI Hub Financial Report

	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Actual YTD	FY24 Encumbered Funds
556002 - CCI - Hub - Labor														
Labor	$424,387	$334,230	$318,739	$317,865	$326,324	$309,975	$333,039	$362,821	$339,163	$312,485	$321,959	$161,937	$3,862,924	
Graduate Tuition Remission						$ 28,586				$100,566		$ 4,219	$133,371	
ECE GRAs (556101)	$43,461	$ 29,115	$31,208	$124,367	$32,183	$ 30,574	$ (6,570)	$ 6,570					$290,908	
Subtotal	**$467,848**	**$363,345**	**$349,947**	**$442,232**	**$358,507**	**$369,135**	**$326,469**	**$369,391**	**$339,163**	**$413,051**	**$321,959**	**$166,156**	**$4,287,203**	**$ -**
Burn Rate	**11%**	**20%**	**29%**	**40%**	**48%**	**58%**	**66%**	**75%**	**83%**	**93%**	**101%**	**105%**	**105%**	
556003 - CCI - Hub - Facilities														
Labor							$ 8,298	$ (8,298)					$ -	
Subtotal													**$ -**	**$ -**
556004 - Hub Operations														
NCR Communications (IT/Servers)	$ 1,488	$ 1,488	$10,031	$ 13,140			$ 14,628		$ 1,488		$ 10,194		$ 52,457	
Copy/Print				$ 2,142	$ 547	$ 323	$ 591		$ 456	$ 526	$ 514	$ 549	$ 5,647	
Travel - Ops Staff (Jenny, John, Alex, Luiz, Laura)	$ 117	$ 770	$ 129	$ 5,622	$ 6,015	$ 594	$ 642	$ 1,622	$ 595	$ 6,505	$ 4,590	$ 6,087	$ 33,287	$ 2,805
Supplies		$ 112	$ 32	$ 144			$ 179	$ 64	$ 62	$ 101	$ 118	$ 22	$ 834	
HR Expenses							$ 960	$ 700					$ 1,660	
VTRC-A Rent	$39,819	$ 39,819	$49,120	$ 39,819	$39,818	$ 39,818	$ 39,818	$ 39,818	$39,818	$ 39,818	$ 39,818	$ 39,818	$487,123	
Misc. Operating Expenses	$ 156	$ 489	$ 2,296	$ 4,691	$ 119	$ (361)	$ 804	$ 12,446	$ 3,492	$ 4,185	$ 821	$ 389	$ 29,528	$ 500
Tuition Reimbursement						$ 1,293			$ 1,293		$ 1,293		$ 3,879	
Meetings (TAB, srsRAN Workshop, NTIA Celebration, Belgium)			$ 1,940		$11,511	$ (10,939)	$ 300					$ 5,939	$ 8,752	
Subtotal	**$41,580**	**$42,678**	**$63,547**	**$65,558**	**$58,010**	**$ 30,728**	**$ 57,923**	**$54,650**	**$47,205**	**$ 51,135**	**$57,348**	**$52,805**	**$623,167**	**$ 3,305**
Burn Rate	**6%**	**13%**	**22%**	**32%**	**41%**	**46%**	**55%**	**63%**	**70%**	**78%**	**87%**	**95%**	**95%**	
556005 - Hub Communications														
Publications & Info Graphics		$ 123	$ 746	$ 159		$ 3,690	$ 5,101	$ 7,642	$ 21				$ 17,482	
Website							$ 23						$ 23	
Branding	$ 474	$ 641			$ 1,332					$ 573			$ 3,020	
Marketing & Social Media Software	$ 151	$ 271		$ 642	$ 271	$ 288	$ 298	$ 288	$ 288	$ 360	$ 288	$ 288	$ 3,433	
Video & Photo			$ 2,500	$ 175				$ 1,562			$ 800		$ 5,037	
Travel - Comms Staff (Michele, Aubrey, Lisa, Intern)								$ 314					$ 314	
Misc Communications Expenses						$ 2,229		$ 8,167	$10,000				$ 20,397	
Subtotal	**$ 625**	**$ 1,035**	**$ 3,246**	**$ 976**	**$ 1,603**	**$ 6,207**	**$ 5,422**	**$17,973**	**$10,309**	**$ 933**	**$ 1,088**	**$ 288**	**$ 49,705**	**$ -**
Burn Rate	**1%**	**4%**	**11%**	**14%**	**17%**	**31%**	**44%**	**85%**	**109%**	**111%**	**114%**	**114%**	**114%**	
556006 - Hub Workforce Dev & Innov+Comm														
Experiential Learning Program												$684,099	$684,099	
CCI Incubator Support (CATAPULT)													$ -	$ 300,000
Hub-led Workforce Development Program					$10,000	$ 10,000							$ 20,000	$ 14,777
Internship Fair							$ 2,500						$ 2,500	
Cyber Fusion					$20,000								$ 20,000	
Inclusion and Accessibility Grants											$300,000		$300,000	
Project Based Learning				$ 16,946									$ 16,946	
Meetup to Startup		$ 612		$ 4,108		$ 427							$ 5,147	
Program Management						$ 25							$ 25	
2024 Commonwealth Cyber Cup Sponsorship								$ 600					$ 600	
Travel - Workforce Staff (Sarah, Kendall, Austin)				$ 1,446	$ 3,870			$ 856	$ 939	$ 2,119			$ 9,230	
Misc Workforce Dev + Innov Expenses	$ 60												$ 60	
Subtotal	**$ 60**	**$ 612**	**$ -**	**$22,499**	**$33,870**	**$ 10,452**	**$ 2,500**	**$ 1,456**	**$ 939**	**$ 2,119**	**$300,000**	**$684,099**	**$1,058,607**	**$ 314,777**
Burn Rate	**0%**	**0%**	**0%**	**2%**	**5%**	**6%**	**6%**	**6%**	**6%**	**6%**	**31%**	**88%**	**88%**	



Appendix 3 FY24 Financial Reports

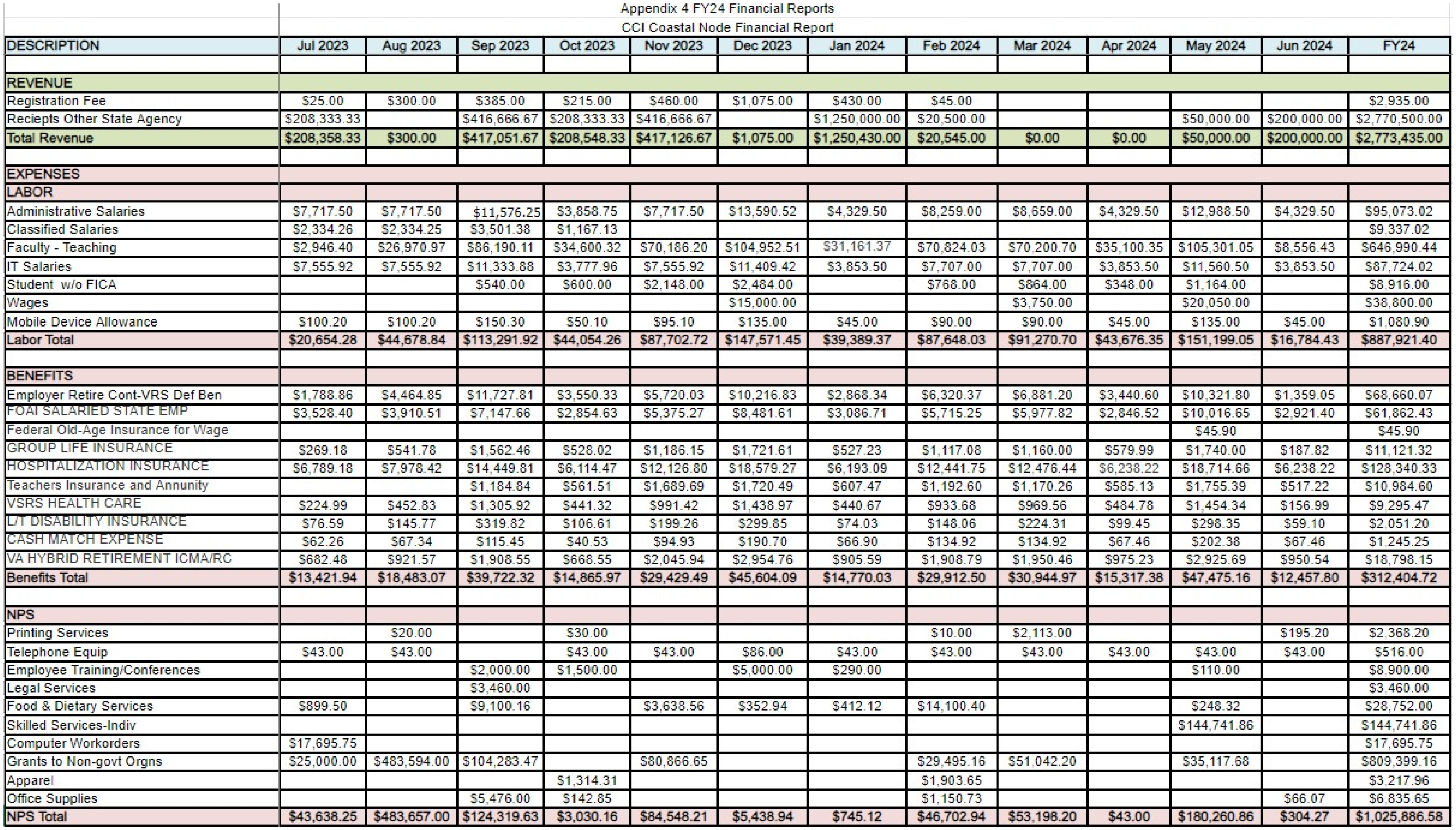
CCI Hub Financial Report

	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Actual YTD	FY24 Encumbered Funds
556007 - Hub Network & External Engagements														
CCI Symposium (Incl. Travel)						$ 1,505	$ 5,650	$ 639		$ 55,233	$ 4,466	$ 3	$ 67,496	$ 10,000
Symposium Registration Revenue								$ (4,950)	$ (7,701)	$ (330)			$ (12,981)	
Symposium Travel										$ 2,148	$ 4,187		$ 6,335	
Virginia Cybersecurity Students (VCyS)								$ 20,500					$ 20,500	
Travel Grants												$ 31,523	$ 31,523	
Catering & Visitor Support	$ 2,020			$ 2,307	$ 626				$ 853				$ 5,806	
Startup Package - Shin'ichiro	$16,150												$ 16,150	
Subtotal	$18,170	$ -	$ -	$ 2,307	$ 626	$ 1,505	$ 5,650	$16,189	$(6,848)	$ 57,051	$ 8,653	$31,526	$134,829	$ 10,000
Burn Rate	5%	5%	5%	6%	6%	7%	8%	13%	11%	27%	30%	39%	39%	
556008 - Hub Research														
Hub Sponsored Research Program - Fall							$649,849						$649,849	
Pres PostDoc Prof Dev		$625											$ 625	
Publication Fees			$1,664	$220	$2,200								$ 4,084	
Travel - Research Expenses		$438	$6,551	$11,625	$8,738	$3,428	$675		$2,879	$1,554	$839	$884	$ 37,611	
Business Meals				$120									$ 120	
Labor									$1,350	$(1,350)			$ -	
Misc Research Expenses	$1,064	$2,304	$4,116	$2,851		$2,560	$3,591		$100		$560		$ 17,147	$489
Subtotal	$ 1,064	$ 3,368	$12,331	$14,816	$10,938	$ 5,988	$654,115	$ -	$ 4,329	$ 204	$ 1,399	$ 884	$709,436	$ 489
Burn Rate	0%	0%	2%	3%	5%	5%	76%	76%	76%	76%	76%	76%	76%	
556009 - Hub Research Infrastructure														
Testbed Software		$ 73								$ 7,045	$ 58		$ 7,175	
Equipment and Supplies	$ 2,733	$ 925		$ 1,436	$ 692	$ (588)			$13,309	$ 2,717	$ 424	$ 129	$ 21,777	$ 19,631
Phone	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 52	$ 627	
Memberships						$ 2,500							$ 2,500	
Subtotal	$ 2,785	$ 1,050	$ 52	$ 1,489	$ 744	$ 1,964	$ 52	$ 52	$13,361	$ 9,815	$ 533	$ 181	$ 32,080	$ 19,631
Burn Rate	1%	2%	2%	2%	3%	4%	4%	4%	9%	14%	14%	14%	14%	
FY24 Total Executed and Encumbered	$532,132	$412,089	$429,124	$549,877	$464,299	$425,979	$1,052,132	$459,711	$408,457	$534,308	$690,980	$935,940	$6,895,026	$ 348,202
FY24 Burn Rate	7%	13%	18%	26%	32%	38%	52%	58%	63%	70%	79%	92%	92%	5%
														FY24 Total Burn Rate
														97%

Appendix 3 FY24 Financial Reports

CCI Central Node Financial Report

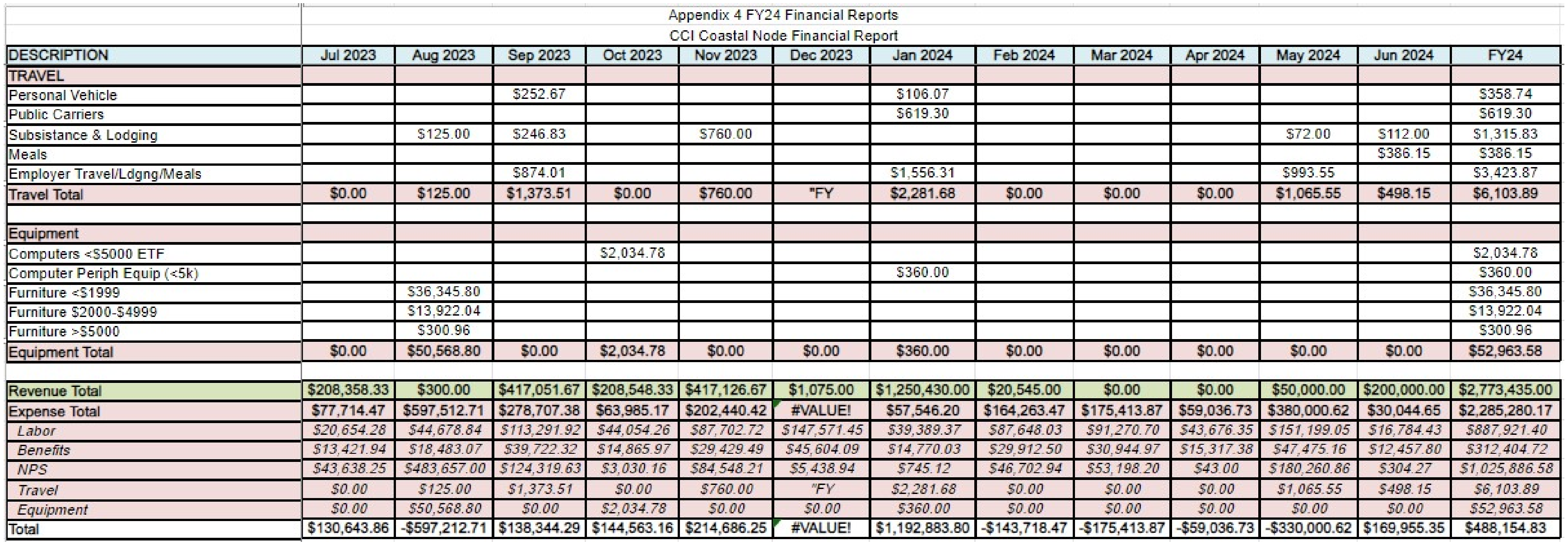
	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Actual YTD	Budget Balance YTD	Budgeted	FY24 Encumbered Funds YTD
Operations																
Personnel	$ -	$ -	$ -	$ -	$ -	$ -	$ 125,000	$ -	$ -	$ 5,167	$ 22,715	$ 9,305	$162,187	$ 242,813	$ 405,000	
CVN Operations	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 87	$ 15,695	$ -	$ 15,781	$ 34,219	$ 50,000	
CVN Partnerships	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 100,000	$ 100,000	
Community Outreach/Events	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 50,000	$ 50,000	
Subtotal	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 125,000**	**$ -**	**$ -**	**$ 5,254**	**$ 38,409**	**$ 9,305**	**$177,968**	**$ 427,032**	**$605,000**	**$ -**
Burn Rate	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**21%**	**21%**	**21%**	**22%**	**28%**	**29%**	**29%**			
Workforce Development																
Experiential Learning CFP	$ -	$ -	$ -	$ -	$ -	$ -	$ 100,000	$ 110,000	$ -			$ -	$210,000	$ 30,000	$ 240,000	
Interships in CVN	$ -	$ -	$ -	$ -	$ -	$ -	$ 75,000	$ -	$ -			$ -	$ 75,000	$ 75,000	$ 150,000	
Subtotal	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 175,000**	**$ 110,000**	**$ -**	**$ -**	**$ -**	**$ -**	**$285,000**	**$ 105,000**	**$390,000**	**$ -**
Burn Rate	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**45%**	**73%**	**73%**	**73%**	**73%**	**73%**	**73%**			
Regional Innovation & Commercialization																
Innovation to CVN	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 20,000	$ 20,000	
Innovation to VCU	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 55,000	$ 55,000	
Innovation to UVA	$ -	$ -	$ -	$ -	$ -	$ -	$ 55,000	$ -	$ -	$ -	$ -	$ -	$ 55,000	$ -	$ 55,000	
Subtotal	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 55,000**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$55,000**	**$ 75,000**	**$130,000**	**$ -**
Burn Rate	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**42%**	**42%**	**42%**	**42%**	**42%**	**42%**	**42%**			
Research & Investment																
Support Existing Programs	$ -	$ -	$ -	$ -	$ -	$ -	$ 150,000	$ 7,754	$ 12,341	$ 25,742	$ 3,929	$ 22,268	$222,033	$ 227,967	$ 450,000	
Research Faculty	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ 1,188	$ -	$ -	$ -	$ 1,188	$ 123,812	$ 125,000	
Research CFPs	$ -	$ -	$ -	$ -	$ -	$ -	$ 300,000	$ 500,000	$ -				$800,000	$ -	$ 800,000	
Subtotal	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 450,000**	**$ 507,754**	**$ 13,529**	**$ 25,742**	**$ 3,929**	**$ 22,268**	**$1,023,221**	**$ 351,779**	**$1,375,000**	**$ -**
Burn Rate	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**33%**	**70%**	**71%**	**73%**	**73%**	**74%**	**74%**			
FY24 Total Executed and Encumbered	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ 805,000**	**$ 617,754**	**$ 13,529**	**$ 30,996**	**$ 42,338**	**$ 31,573**	**$1,541,189**	**$ 958,811**	**$2,500,000**	**$ -**
FY24 Burn Rate	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**32%**	**57%**	**57%**	**59%**	**60%**	**62%**	**62%**			



Appendix 4 FY24 Financial Reports

CCI Coastal Node Financial Report

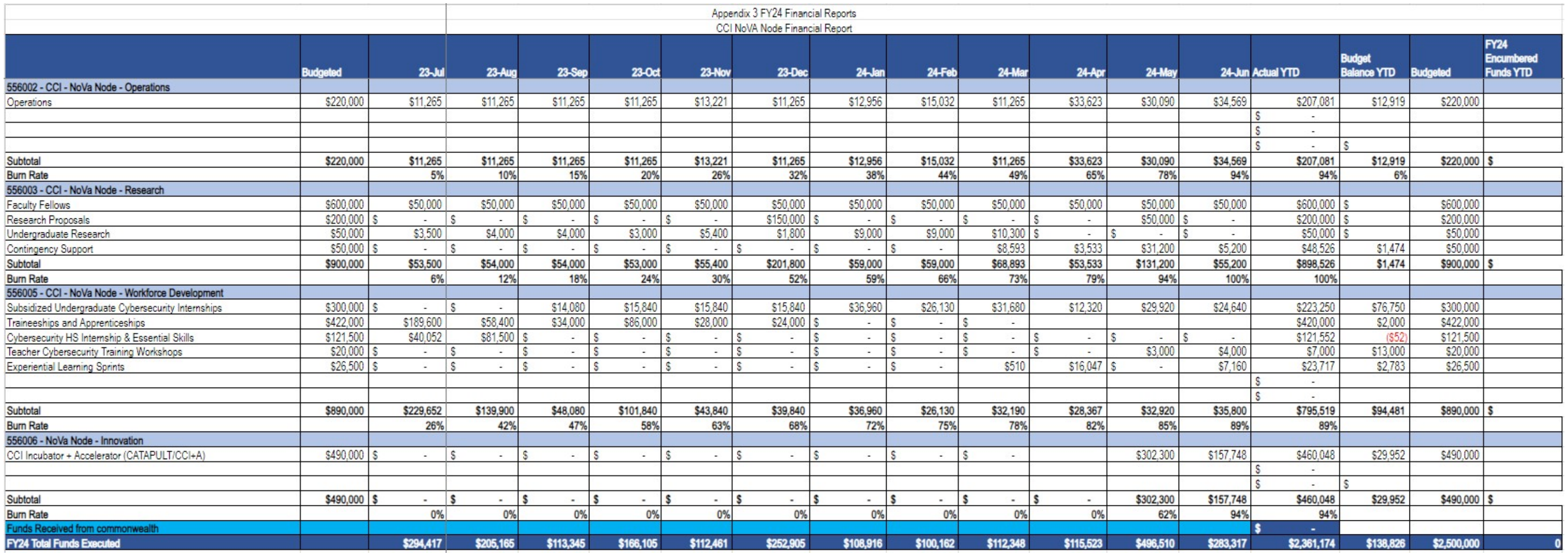
DESCRIPTION	Jul 2023	Aug 2023	Sep 2023	Oct 2023	Nov 2023	Dec 2023	Jan 2024	Feb 2024	Mar 2024	Apr 2024	May 2024	Jun 2024	FY24
REVENUE													
Registration Fee	$25.00	$300.00	$385.00	$215.00	$460.00	$1,075.00	$430.00	$45.00					$2,935.00
Reciepts Other State Agency	$208,333.33		$416,666.67	$208,333.33	$416,666.67		$1,250,000.00	$20,500.00			$50,000.00	$200,000.00	$2,770,500.00
Total Revenue	$208,358.33	$300.00	$417,051.67	$208,548.33	$417,126.67	$1,075.00	$1,250,430.00	$20,545.00	$0.00	$0.00	$50,000.00	$200,000.00	$2,773,435.00
EXPENSES													
LABOR													
Administrative Salaries	$7,717.50	$7,717.50	$11,576.25	$3,858.75	$7,717.50	$13,590.52	$4,329.50	$8,259.00	$8,659.00	$4,329.50	$12,988.50	$4,329.50	$95,073.02
Classified Salaries	$2,334.26	$2,334.25	$3,501.38	$1,167.13									$9,337.02
Faculty - Teaching	$2,946.40	$26,970.97	$86,190.11	$34,600.32	$70,186.20	$104,952.51	$31,161.37	$70,824.03	$70,200.70	$35,100.35	$105,301.05	$8,556.43	$646,990.44
IT Salaries	$7,555.92	$7,555.92	$11,333.88	$3,777.96	$7,555.92	$11,409.42	$3,853.50	$7,707.00	$7,707.00	$3,853.50	$11,560.50	$3,853.50	$87,724.02
Student w/o FICA			$540.00	$600.00	$2,148.00	$2,484.00		$768.00	$864.00	$348.00	$1,164.00		$8,916.00
Wages						$15,000.00			$3,750.00		$20,050.00		$38,800.00
Mobile Device Allowance	$100.20	$100.20	$150.30	$50.10	$95.10	$135.00	$45.00	$90.00	$90.00	$45.00	$135.00	$45.00	$1,080.90
Labor Total	$20,654.28	$44,678.84	$113,291.92	$44,054.26	$87,702.72	$147,571.45	$39,389.37	$87,648.03	$91,270.70	$43,676.35	$151,199.05	$16,784.43	$887,921.40
BENEFITS													
Employer Retire Cont-VRS Def Ben	$1,788.86	$4,464.85	$11,727.81	$3,550.33	$5,720.03	$10,216.83	$2,868.34	$6,320.37	$6,881.20	$3,440.60	$10,321.80	$1,359.05	$68,660.07
FOAI SALARIED STATE EMP	$3,528.40	$3,910.51	$7,147.66	$2,854.63	$5,375.27	$8,481.61	$3,086.71	$5,715.25	$5,977.82	$2,846.52	$10,016.65	$2,921.40	$61,862.43
Federal Old-Age Insurance for Wage											$45.90		$45.90
GROUP LIFE INSURANCE	$269.18	$541.78	$1,562.46	$528.02	$1,186.15	$1,721.61	$527.23	$1,117.08	$1,160.00	$579.99	$1,740.00	$187.82	$11,121.32
HOSPITALIZATION INSURANCE	$6,789.18	$7,978.42	$14,449.81	$6,114.47	$12,126.80	$18,579.27	$6,193.09	$12,441.75	$12,476.44	$6,238.22	$18,714.66	$6,238.22	$128,340.33
Teachers Insurance and Annunity			$1,184.84	$561.51	$1,689.69	$1,720.49	$607.47	$1,192.60	$1,170.26	$585.13	$1,755.39	$517.22	$10,984.60
VSRS HEALTH CARE	$224.99	$452.83	$1,305.92	$441.32	$991.42	$1,438.97	$440.67	$933.68	$969.56	$484.78	$1,454.34	$156.99	$9,295.47
L/T DISABILITY INSURANCE	$76.59	$145.77	$319.82	$106.61	$199.26	$299.85	$74.03	$148.06	$224.31	$99.45	$298.35	$59.10	$2,051.20
CASH MATCH EXPENSE	$62.26	$67.34	$115.45	$40.53	$94.93	$190.70	$66.90	$134.92	$134.92	$67.46	$202.38	$67.46	$1,245.25
VA HYBRID RETIREMENT ICMA/RC	$682.48	$921.57	$1,908.55	$668.55	$2,045.94	$2,954.76	$905.59	$1,908.79	$1,950.46	$975.23	$2,925.69	$950.54	$18,798.15
Benefits Total	$13,421.94	$18,483.07	$39,722.32	$14,865.97	$29,429.49	$45,604.09	$14,770.03	$29,912.50	$30,944.97	$15,317.38	$47,475.16	$12,457.80	$312,404.72
NPS													
Printing Services		$20.00		$30.00				$10.00	$2,113.00			$195.20	$2,368.20
Telephone Equip	$43.00	$43.00		$43.00	$43.00	$86.00	$43.00	$43.00	$43.00	$43.00	$43.00	$43.00	$516.00
Employee Training/Conferences			$2,000.00	$1,500.00		$5,000.00	$290.00				$110.00		$8,900.00
Legal Services			$3,460.00										$3,460.00
Food & Dietary Services	$899.50		$9,100.16		$3,638.56	$352.94	$412.12	$14,100.40			$248.32		$28,752.00
Skilled Services-Indiv											$144,741.86		$144,741.86
Computer Workorders	$17,695.75												$17,695.75
Grants to Non-govt Orgns	$25,000.00	$483,594.00	$104,283.47		$80,866.65			$29,495.16	$51,042.20		$35,117.68		$809,399.16
Apparel				$1,314.31				$1,903.65					$3,217.96
Office Supplies			$5,476.00	$142.85				$1,150.73				$66.07	$6,835.65
NPS Total	$43,638.25	$483,657.00	$124,319.63	$3,030.16	$84,548.21	$5,438.94	$745.12	$46,702.94	$53,198.20	$43.00	$180,260.86	$304.27	$1,025,886.58



Appendix 4 FY24 Financial Reports

CCI Coastal Node Financial Report

DESCRIPTION	Jul 2023	Aug 2023	Sep 2023	Oct 2023	Nov 2023	Dec 2023	Jan 2024	Feb 2024	Mar 2024	Apr 2024	May 2024	Jun 2024	FY24
TRAVEL													
Personal Vehicle			$252.67				$106.07						$358.74
Public Carriers							$619.30						$619.30
Subsistance & Lodging		$125.00	$246.83		$760.00						$72.00	$112.00	$1,315.83
Meals												$386.15	$386.15
Employer Travel/Ldgng/Meals			$874.01				$1,556.31				$993.55		$3,423.87
Travel Total	$0.00	$125.00	$1,373.51	$0.00	$760.00	"FY	$2,281.68	$0.00	$0.00	$0.00	$1,065.55	$498.15	$6,103.89
Equipment													
Computers <$5000 ETF				$2,034.78									$2,034.78
Computer Periph Equip (<5k)							$360.00						$360.00
Furniture <$1999		$36,345.80											$36,345.80
Furniture $2000-$4999		$13,922.04											$13,922.04
Furniture >$5000		$300.96											$300.96
Equipment Total	$0.00	$50,568.80	$0.00	$2,034.78	$0.00	$0.00	$360.00	$0.00	$0.00	$0.00	$0.00	$0.00	$52,963.58
Revenue Total	$208,358.33	$300.00	$417,051.67	$208,548.33	$417,126.67	$1,075.00	$1,250,430.00	$20,545.00	$0.00	$0.00	$50,000.00	$200,000.00	$2,773,435.00
Expense Total	$77,714.47	$597,512.71	$278,707.38	$63,985.17	$202,440.42	#VALUE!	$57,546.20	$164,263.47	$175,413.87	$59,036.73	$380,000.62	$30,044.65	$2,285,280.17
Labor	*$20,654.28*	*$44,678.84*	*$113,291.92*	*$44,054.26*	*$87,702.72*	*$147,571.45*	*$39,389.37*	*$87,648.03*	*$91,270.70*	*$43,676.35*	*$151,199.05*	*$16,784.43*	*$887,921.40*
Benefits	*$13,421.94*	*$18,483.07*	*$39,722.32*	*$14,865.97*	*$29,429.49*	*$45,604.09*	*$14,770.03*	*$29,912.50*	*$30,944.97*	*$15,317.38*	*$47,475.16*	*$12,457.80*	*$312,404.72*
NPS	*$43,638.25*	*$483,657.00*	*$124,319.63*	*$3,030.16*	*$84,548.21*	*$5,438.94*	*$745.12*	*$46,702.94*	*$53,198.20*	*$43.00*	*$180,260.86*	*$304.27*	*$1,025,886.58*
Travel	*$0.00*	*$125.00*	*$1,373.51*	*$0.00*	*$760.00*	*"FY*	*$2,281.68*	*$0.00*	*$0.00*	*$0.00*	*$1,065.55*	*$498.15*	*$6,103.89*
Equipment	*$0.00*	*$50,568.80*	*$0.00*	*$2,034.78*	*$0.00*	*$0.00*	*$360.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$0.00*	*$52,963.58*
Total	$130,643.86	-$597,212.71	$138,344.29	$144,563.16	$214,686.25	#VALUE!	$1,192,883.80	-$143,718.47	-$175,413.87	-$59,036.73	-$330,000.62	$169,955.35	$488,154.83



Appendix 3 FY24 Financial Reports

CCI NoVA Node Financial Report

	Budgeted	23-Jul	23-Aug	23-Sep	23-Oct	23-Nov	23-Dec	24-Jan	24-Feb	24-Mar	24-Apr	24-May	24-Jun	Actual YTD	Budget Balance YTD	Budgeted	FY24 Encumbered Funds YTD
556002 - CCI - NoVa Node - Operations																	
Operations	$220,000	$11,265	$11,265	$11,265	$11,265	$13,221	$11,265	$12,956	$15,032	$11,265	$33,623	$30,090	$34,569	$207,081	$12,919	$220,000	
														$ -			
														$ -			
														$ -	$		
Subtotal	**$220,000**	**$11,265**	**$11,265**	**$11,265**	**$11,265**	**$13,221**	**$11,265**	**$12,956**	**$15,032**	**$11,265**	**$33,623**	**$30,090**	**$34,569**	**$207,081**	**$12,919**	**$220,000**	**$**
Burn Rate		**5%**	**10%**	**15%**	**20%**	**26%**	**32%**	**38%**	**44%**	**49%**	**65%**	**78%**	**94%**	**94%**	**6%**		
556003 - CCI - NoVa Node - Research																	
Faculty Fellows	$600,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$50,000	$600,000	$	$600,000	
Research Proposals	$200,000	$ -	$ -	$ -	$ -	$ -	$150,000	$ -	$ -	$ -	$ -	$50,000	$ -	$200,000	$	$200,000	
Undergraduate Research	$50,000	$3,500	$4,000	$4,000	$3,000	$5,400	$1,800	$9,000	$9,000	$10,300	$ -	$ -	$ -	$50,000	$	$50,000	
Contingency Support	$50,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$8,593	$3,533	$31,200	$5,200	$48,526	$1,474	$50,000	
Subtotal	**$900,000**	**$53,500**	**$54,000**	**$54,000**	**$53,000**	**$55,400**	**$201,800**	**$59,000**	**$59,000**	**$68,893**	**$53,533**	**$131,200**	**$55,200**	**$898,526**	**$1,474**	**$900,000**	**$**
Burn Rate		**6%**	**12%**	**18%**	**24%**	**30%**	**52%**	**59%**	**66%**	**73%**	**79%**	**94%**	**100%**	**100%**			
556005 - CCI - NoVa Node - Workforce Development																	
Subsidized Undergraduate Cybersecurity Internships	$300,000	$ -	$ -	$14,080	$15,840	$15,840	$15,840	$36,960	$26,130	$31,680	$12,320	$29,920	$24,640	$223,250	$76,750	$300,000	
Traineeships and Apprenticeships	$422,000	$189,600	$58,400	$34,000	$86,000	$28,000	$24,000	$ -	$ -	$ -				$420,000	$2,000	$422,000	
Cybersecurity HS Internship & Essential Skills	$121,500	$40,052	$81,500	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$121,552	($52)	$121,500	
Teacher Cybersecurity Training Workshops	$20,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$3,000	$4,000	$7,000	$13,000	$20,000	
Experiential Learning Sprints	$26,500	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$510	$16,047	$ -	$7,160	$23,717	$2,783	$26,500	
														$ -			
														$ -			
Subtotal	**$890,000**	**$229,652**	**$139,900**	**$48,080**	**$101,840**	**$43,840**	**$39,840**	**$36,960**	**$26,130**	**$32,190**	**$28,367**	**$32,920**	**$35,800**	**$795,519**	**$94,481**	**$890,000**	**$**
Burn Rate		**26%**	**42%**	**47%**	**58%**	**63%**	**68%**	**72%**	**75%**	**78%**	**82%**	**85%**	**89%**	**89%**			
556006 - NoVa Node - Innovation																	
CCI Incubator + Accelerator (CATAPULT/CCI+A)	$490,000	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -	$ -		$302,300	$157,748	$460,048	$29,952	$490,000	
														$ -			
														$ -	$		
Subtotal	**$490,000**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$ -**	**$302,300**	**$157,748**	**$460,048**	**$29,952**	**$490,000**	**$**
Burn Rate		**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**0%**	**62%**	**94%**	**94%**			
Funds Received from commonwealth														**$ -**			
FY24 Total Funds Executed		**$294,417**	**$205,165**	**$113,345**	**$166,105**	**$112,461**	**$252,905**	**$108,916**	**$100,162**	**$112,348**	**$115,523**	**$496,510**	**$283,317**	**$2,361,174**	**$138,826**	**$2,500,000**	**0**

Appendix 4 FY24 Financial Reports

CCI Southwest Node Financial Report

	Jul-23	Aug-23	Sep-23	Oct-23	Nov-23	Dec-23	Jan-24	Feb-24	Mar-24	Apr-24	May-24	Jun-24	Actual YTD	Budget Balance YTD
556020 - CCI SWVA - Node Research														
Research Projects		$ 50,000.00		$847,500.00			$ 155,000.00					$ 94,000.00	$1,146,500.00	$ 53,500.00
Research Personnel	$ 6,656.63	$123,450.30	$ 13,217.59	$104,667.59	$ 5,867.84	$ 4,314.90	$ 39,738.22	$ 4,746.44	$ 4,536.76		$ 30,000.00		$337,196.27	$ 32,803.73
Other													$ -	$ -
													$ -	$ -
Subtotal	**$ 6,656.63**	**$173,450.30**	**$13,217.59**	**$952,167.59**	**$ 5,867.84**	**$ 4,314.90**	**$194,738.22**	**$ 4,746.44**	**$ 4,536.76**	**$ -**	**$ 30,000.00**	**$ 94,000.00**	**$1,483,696.27**	**$ 86,303.73**
Burn Rate	**0%**	**11%**	**12%**	**73%**	**73%**	**74%**	**86%**	**86%**	**87%**	**87%**	**89%**	**95%**	**95%**	
556021 - CCI SWVA - Node Innovation and Talent Pipelir														
Innovation Projects				$100,000.00			$ 50,000.00				$ 62,000.00		$212,000.00	$ 8,000.00
Workforce Projects		$ 68,000.00	$ 18,000.00	$ 3,642.00			$ 1,000.00		$ 8,532.00	$ 61,426.00	$ 85,500.00	$159,465.00	$405,565.00	$ 4,435.00
Innovation Personnel	$ 2,500.00				$ 8,000.00						$ 2,500.00		$ 13,000.00	$ -
Outreach costs			$ 1,029.32	$ 1,621.69	$ 388.80	$ 659.55	$ 1,500.00		$ 2,911.06	$ 197.40	$ 5,000.00		$ 13,307.82	$ 1,692.18
Internal CCI SWVA Interns			$ 1,086.84	$ 1,331.64	$ 1,586.52	$ 1,239.83	$ -	$ 1,048.47	$ 422.03	$ 1,251.42	$ 735.73		$ 8,702.48	$ 297.52
Other													$ -	$ -
Subtotal	**$ 2,500.00**	**$ 68,000.00**	**$20,116.16**	**$106,595.33**	**$ 9,975.32**	**$ 1,899.38**	**$ 52,500.00**	**$ 1,048.47**	**$11,865.09**	**$ 62,874.82**	**$155,735.73**	**$159,465.00**	**$652,575.30**	**$ 14,424.70**
Burn Rate	**0%**	**11%**	**14%**	**30%**	**31%**	**31%**	**39%**	**39%**	**41%**	**51%**	**74%**	**98%**	**98%**	
556022 - CCI SWVA - Node Operations														
Labor	$ 26,583.00	$ 57,622.09	$ 17,781.24	$ 17,781.25	$ 18,696.47	$ 17,231.36	$ 18,248.48	$ 18,256.70	$ 18,047.01	$ 13,406.57	$ 13,408.71	$ 6,704.34	$243,767.22	$ 6,232.78
Telecom	$ 122.25	$ 219.25	$ 685.09	$ 92.24	$ 112.25	$ 112.25	$ 112.25	$ 112.25	$ 112.25	$ 112.25	$ 112.25	$ 112.25	$ 2,016.83	$ (16.83)
Operating costs			$ 24.00	$ 715.66	$ 327.92	$ 75.70			$ 984.96	$ 163.54		$ 111.45	$ 2,403.23	$ 1,596.77
Travel and Training Costs			$ 792.17	$ 1,869.97	$ 1,200.43	$ 210.00			$ 524.63	$ 2,054.76			$ 6,651.96	$ 348.04
													$ -	
Subtotal	**$26,705.25**	**$ 57,841.34**	**$19,282.50**	**$ 20,459.12**	**$20,337.07**	**$ 17,629.31**	**$ 18,360.73**	**$ 18,368.95**	**$19,668.85**	**$ 15,737.12**	**$ 13,520.96**	**$ 6,928.04**	**$254,839.24**	**$ 8,160.76**
Burn Rate	**10%**	**32%**	**39%**	**47%**	**55%**	**62%**	**69%**	**76%**	**83%**	**89%**	**94%**	**97%**	**97%**	
FY24 Total Executed and Encumbered	**$35,861.88**	**$299,291.64**	**$52,616.25**	**$1,079,222.04**	**$36,180.23**	**$ 23,843.59**	**$265,598.95**	**$ 24,163.86**	**$36,070.70**	**$ 78,611.94**	**$199,256.69**	**$260,393.04**	**$2,391,110.81**	**$ 108,889.19**
FY24 Burn Rate	**1%**	**13%**	**16%**	**59%**	**60%**	**61%**	**72%**	**73%**	**74%**	**77%**	**85%**	**96%**	**96%**	

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/