Fiscal Year 2023 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 2023 REPORT

Commonwealth Cyber Initiative

September 29, 2023

Message from the Executive Director

The Commonwealth of Virginia is the only state in the nation to have a cybersecurity initiative of the scope of the Commonwealth Cyber Initiative (CCI), with interlocking missions of research, innovation, and workforce development.

This year, we commissioned the second study on the economic impact that CCI has had to date. This study, conducted by RTI International, has revealed that in the last fiscal year CCI has contributed to the creation of 889 jobs in the commonwealth, with a value-add of $100 million to Virginia's GDP.

Our research strategy has paid dramatic dividends: The critical mass achieved in CCI and our focus on enabling Virginia researchers to be more competitive large-scale grants have led to a 115% increase in new research funding for cybersecurity from federal and private sector sources, as compared to the previous three fiscal years. In Fiscal Year 2023 (FY23), CCI researchers brought in $75M in new contracts.

In workforce development, our focus is on providing experiential learning opportunities that retain Virginia students in the cyber workforce, increase their ability to secure good jobs, and contribute to their career satisfaction and success. Hundreds of students have gone through CCI internships, apprenticeships, and other experiential learning programs; testimonies from them and their employers attest to the importance of such programs.

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).

Virginia continues to attract top talent and to build a vibrant cybersecurity ecosystem. We are fortunate to have legislative and executive branches that understand how investment in this critical sector benefits the entire population of the commonwealth, as well as the nation. In this report, you will read about how CCI is helping to build this ecosystem.

Luiz DaSilva, Ph.D.; Fellow, IEEE

Executive Director, Commonwealth Cyber Initiative

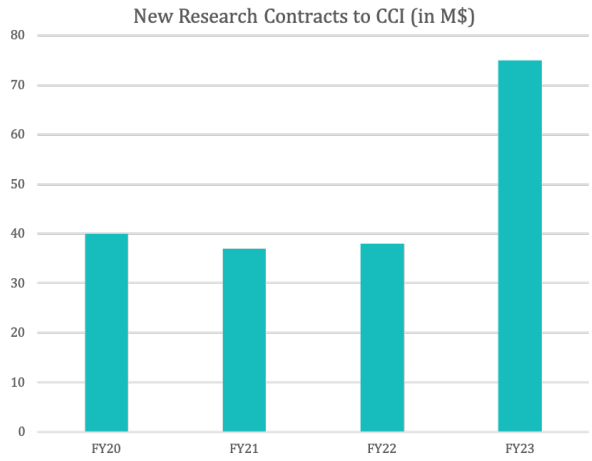
Bradley Professor of Cybersecurity, Virginia Tech

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).

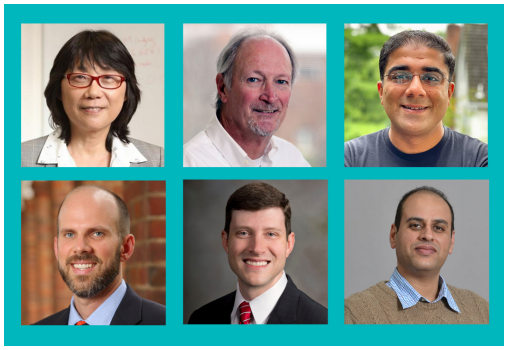
Our ambitious vision is to establish Virginia as a global leader in cybersecurity, and by doing so, help diversify the economy of the commonwealth, attracting private investment and jobs.

Fiscal Year 2023 (FY23) saw a massive 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 42), 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.



Record-breaking Research Funding. In the first three fiscal years that CCI was active, our researchers brought in an average of $35M per year in new research contracts from federal government and private sector sources. These results already resulted in a significant jump in research expenditures in Virginia universities in the area of computer and information science and engineering. In FY23, this total jumped to $75M in new cybersecurity research contracts, an incredible 115% year-to-year increase. Our investments in research infrastructure and collaboration among researchers across CCI universities and disciplines will continue to pay off, especially in areas of opportunity such as Open Radio Access Network (O-RAN), a topic with strong national security implications, for which the recent CHIPS and Science Act has authorized federal funding of $1.5 billion, and in supply chain security, which we have identified as a topic for investment in the coming year.

Focus on Large Grants. CCI creates the critical mass of research expertise for Virginia to be competitive for large research grants. In FY23, our researchers brought in 12 grants of $1M or more; our largest grant, led by George Mason University, was for $29M. Our strategy from the outset has been to enable these large-scale grants, through the CCI Fellows program. This year, we have funded six new Fellows, depicted on the right, at the University of Virginia (UVA), Mason, Virginia Military Institute (VMI), and Virginia Tech (VT). Each received financial support from CCI to lead a research proposal with a budget of $2M or more involving more than one CCI university. A CCI Fellow, funded in Fiscal Year 2020 (FY20) and Fiscal Year 2021 (FY21) under this program, was instrumental in the success in the $29M grant awarded this year.



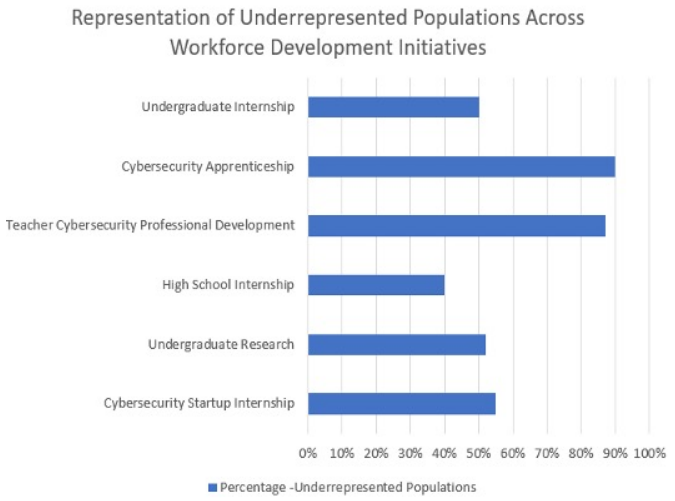
From Lab to Startup. In 2023, CCI continued support for its Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects amongst CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. We have funded nine new ideas, ranging from a multi-functional coating to prevent electromagnetic sabotage (VCU professor Radhika Barua and her team, pictured) to software solutions that protect our systems from social engineering attacks, to mention just a few. 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. 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.

Meet Up to Startup. Speaking of venture capital, this year we began a series of meetups across the commonwealth 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. Virginia-based VCs represented, include: Dreamit Ventures, Data Tribe, Blu Ventures, Squadra, Midland Capital, and Activation Capital. This program is being expanded in FY24, with events already scheduled in Lexington, Fairfax, Harrisonburg, Williamsburg, and Charlotteville.

State of the Art Facilities. CCI's three mission lines of research, innovation, and workforce development all rely on state-of-the-art lab facilities. In FY23, ODU started planning and building their new facilities that will house their School of Data Science, School of Cybersecurity, VMASC, as well as the CCI CoVA Node in the Virginia Beach Town Center. The CCI Central Virginia Node, in partnership with Micron, further developed the OpenCyberCity testbed at VCU, as well as a haptic feedback device prototype. The CCI

Northern Virginia Node maintains open source testbeds at Mason and three commercial-grade NextG systems in its Living Innovation Lab in Arlington, Virginia. The 5G for the Power Grid testbed, depicted, which started as a digital twin of the Virginia Tech Electric Service system, is used for cyber training and for companies to evaluate new technologies before they are deployed in the power system.

A Statewide Experiential Learning Portfolio. Over the past four years, CCI has created a unique and varied portfolio of experiential learning programs for Virginia students. Research shows that such experiences correlate with higher rates of credentialing, success in employment after graduation, higher compensation, and job satisfaction. Our programs range from internships and traineeships to capture-the-flag competitions, intensive training, and project-based learning in partnership with industry leaders in cybersecurity like CACI International. This year, CCI supported 262 interns, the highest number since its inception. Diversifying the cyber workforce has been an explicit goal for us, and all of our programs have participation from women, latinos, and African-Americans at levels greater than in the cybersecurity workforce. As depicted in the plot, 90% of participants in our apprenticeship program come from underrepresented groups.



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 development 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 center.
- Capacity building in Virginia on the topic of supply chain security.
- Leadership in innovation, training, and research in open radio access networks.
- Expansion of international engagements across our three mission lines.
- Continuing to scale up our experiential learning programs.
- New and continuing innovation programs, such as our incubator and accelerator, Meet Up to Startup, and new programs, to strengthen the funding and investment pipeline from ideation to market.

The CCI economic impact study, conducted every two years by RTI International, revealed that in the past two fiscal years, CCI was responsible for the creation of 1,508 jobs in Virginia, corresponding to $119.7 million in labor income, and $214.3 million in value-add to the Virginia Gross Domestic Product (GDP). The return on investment, to date, significantly exceeds the initial expectations set out in the CCI Blueprint five years ago, and continues to grow.

List of Figures

List of Tables

List of Acronyms

3GPP 3rd Generation Partnership Project

5GPG 5G for the Power Grid

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

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

GDP Gross Domestic Product

Mason George Mason University

HR Human Resources

IDC Inclusion & Diversity Committee

IoT Internet of Things

IP Intellectual Property

IUCRC Industry-University Cooperative Research Center

JMU James Madison University

LC Leadership Council

NoVA Northern Virginia

NVCC Northern Virginia Community College

NSF National Science Foundation

ODU Old Dominion University

O-RAN Open Radio Access Network

OTIC Open Testing and Integration Center

PI Principal Investigator

RAN Radio Access Network

RTDS Real Time Digital Simulator

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

VIPA Virginia Innovation Partnership Authority

VIPC Virginia Innovation Partnership Corporation

VMI Virginia Military Institute

VPAC Virginia Power Analytics and Cybersecurity

VPRI Vice President for Research and Innovation

VSGC Virginia Space Grant Consortium

VT Virginia Tech

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

W&M William & Mary

xG Next Generation Networks

Contents

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 FY23, 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 FY23, CCI grew again, with the addition of Blue Ridge Community College, in Weyers Cave, VA, to our network. The CCI network now comprises **42** institutions of higher education across Virginia, depicted in Figure 1.1.

The leadership structure of CCI comprises a hub and four regional nodes. VT serves as the anchoring institution for the hub and coordinates the strategy and activities of the network; the hub is hosted in VT's facilities in Arlington. CCI's Central Virginia Node (CVN) is led by Virginia Commonwealth University (VCU), the Coastal Virginia Node (CoVA) is led by ODU, the Northern Virginia (NoVA) Node is led by Mason, and the Sothwest Virginia Node (SWVA) Node 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.

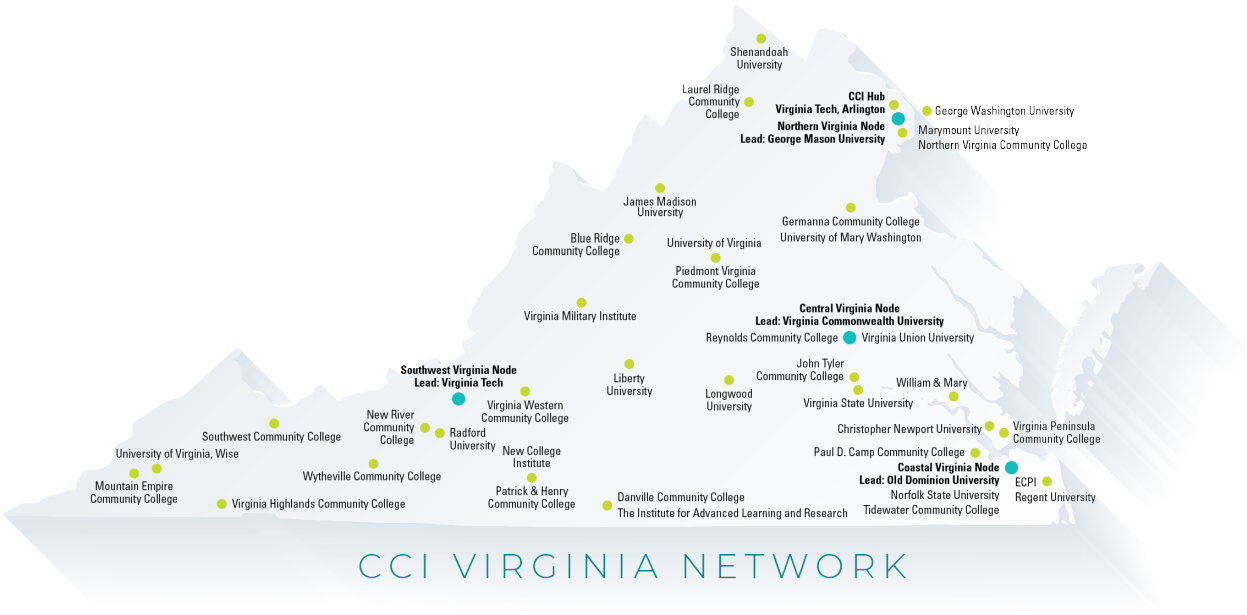


Figure 1.1: The CCI network comprises 42 institutions of higher education across Virginia. Blue Ridge Community College is the latest member to join.

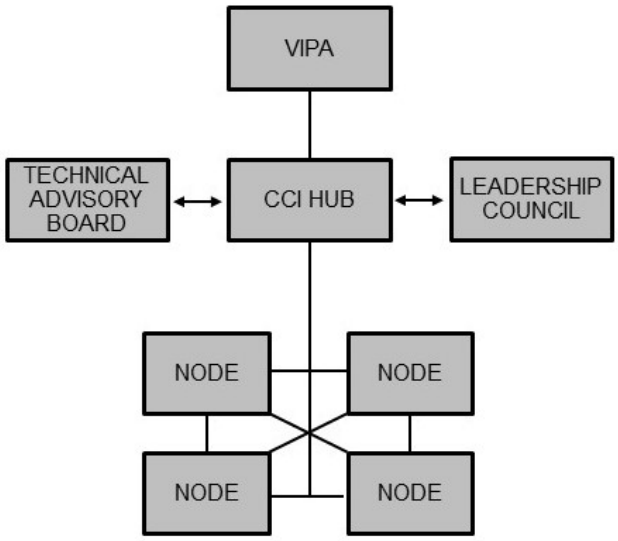


Figure 1.2: CCI governance structure.

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

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

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

Figure 1.3: Roles of the CCI Hub and Nodes.

The CCI executive director, managing director, and the four node directors form the CCI Leadership Council (LC), depicted in Figure 1.4. Dr. Luiz DaSilva serves as 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. Brian Payne serves as CoVA node director; he is also vice provost for Academic Affairs at ODU. Dr. Erdem Topsakal serves as 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 infrastructure in each of the nodes.

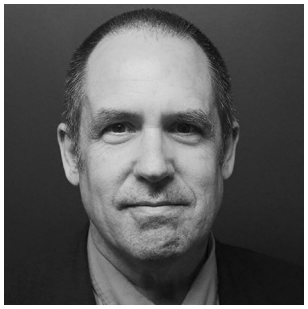
1.2.2 CCI Hub Organization and Research Infrastructure Development

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 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.

(a) Dr. Luiz DaSilva, Executive Director.

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



(c) Dr. Brian Payne, CoVA Node Director.

(d) Dr. Erdem Topsakal, CVN Director.

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

(f) Mr. John Delaney, Managing Director.

Figure 1.4: CCI Leadership Council.

1.2.3 CCI Node Organization and Research Infrastucture Development

Each of the CCI nodes is led by a node director, as depicted in Figure 1.4. The regional nodes have an extremely lean administrative structure, with each node director assisted by a program manager.

In FY23, ODU started planning and building their new facilities that will house their School of Data Science, School of Cybersecurity, VMASC, as well as the CCI CoVA Node in the Virginia Beach Town Center in Fall 2023. The facilities include classrooms, collaborative spaces and state-of-the-art labs, depicted in Figure 1.7. During FY23, $75,000 was put towards purchasing additional equipment to update computer hardware for the CoVA SHARE environment to support ODU graduate courses and Camp Community College students to use virtual machines and simulations to improve their cyber, networking, and program skills in a structured lab. In addition, the CCI CoVA Node enhanced the CASE-V testbed with a Ceph-based software-defined storage infrastructure at Norfolk State University to provide a storage solution that will seamlessly integrate into their current testbed and provide interfaces for multiple storage types within a single cluster.

The CCI Southwest Virginia Node testbed development projects are summarized in Figure 1.8. The Node continued to grow their C-V2X project from FY22 into FY23 with a private 5G network supporting video analytics using camera sensors at the VTTI Smart Road Intersection. In FY23, the SWVA Node further expanded and enhanced: NetSat, a 5G Power Grid testbed, a digital twin of the Virginia Tech Electric Service system, enabling real-time co-simulation of hardware-in-the-loop power systems and communication networks, a SmartFarm Innovation Network for the CCI community to gather around the Virginia Tech CALS farm and Smartfarm Innovation Network testbeds to discuss technology, internet of things, artificial intelligence, data analytics, and cyberbiosecurity in research translation and practice, additional equipment to support Mobile 5G research to measure performance of 5G cellular and newer experimental wireless technologies ranging from a Dell GPU server to four GPS-disciplined Ettus OctoClock timing distribution systems, as well as a Communications IOT in a Box to identify components required to develop an IOT lab, setup the IOT lab with run-time monitors to collect and analyze data and develop analytic tools to co-relate data from multiple devices.

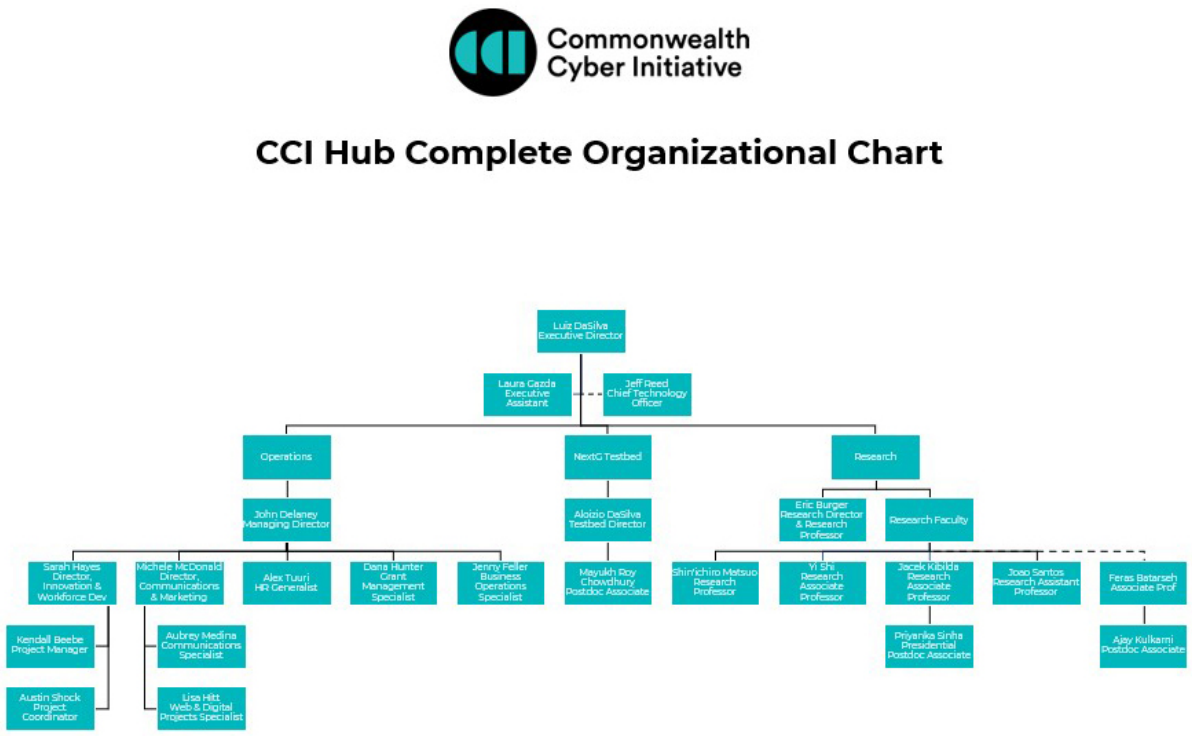


Figure 1.5: CCI organization chart.

The CCI Northern Virginia Node continued to maintain three open source testbeds at George Mason University and three commercial grade functioning NextG Systems in the CCI NoVA Node Living Innovation Lab in Arlington, Virginia. An additional ten Dell EMC R350 Servers, testing equipment, and additional private, commercial-grade 5G networks were added to the NoVa Node Living Innovation Lab in FY23 in addition to existing equipment and infrastructure including a 12x12x10 Anechoic Radio Chamber, timing devices, and O-RAN radios.

In the CCI Central Virginia Node, Virginia Commonwealth University, with Micron, further developed their OpenCyberCity testbed, as well as an initial haptic feedback device prototype, driven using a Texas Instruments DRV2605L to conduct user study experiments and their mapping scheme. Also, Virginia Commonwealth University, in partnership with Sivananthan Labratories, EO Tech, Northrup Grumman, and Leonardo DRS, worked to develop a robust set of sensors for CPS. At the University of Virginia, they developed a wireless federated learning testbed consisting of different edge computing devices. At their Living Link Lab, the University of Virginia purchased a new set of sensors to be deployed across different buldings in engineering to expand the lab platform across multiple buildings. The Medical Device Security (MDS) Testbed in the College of Engineering (CoE) of Virginia Commonwealth University (VCU) is a collaborative research effort between several research labs across disciplines to investigate vulnerabilities in medical devices and their usage. The testbed contains over 40 medical devices on an internal, isolated network configured for testing, and numerous commercial tools for investigation.

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:

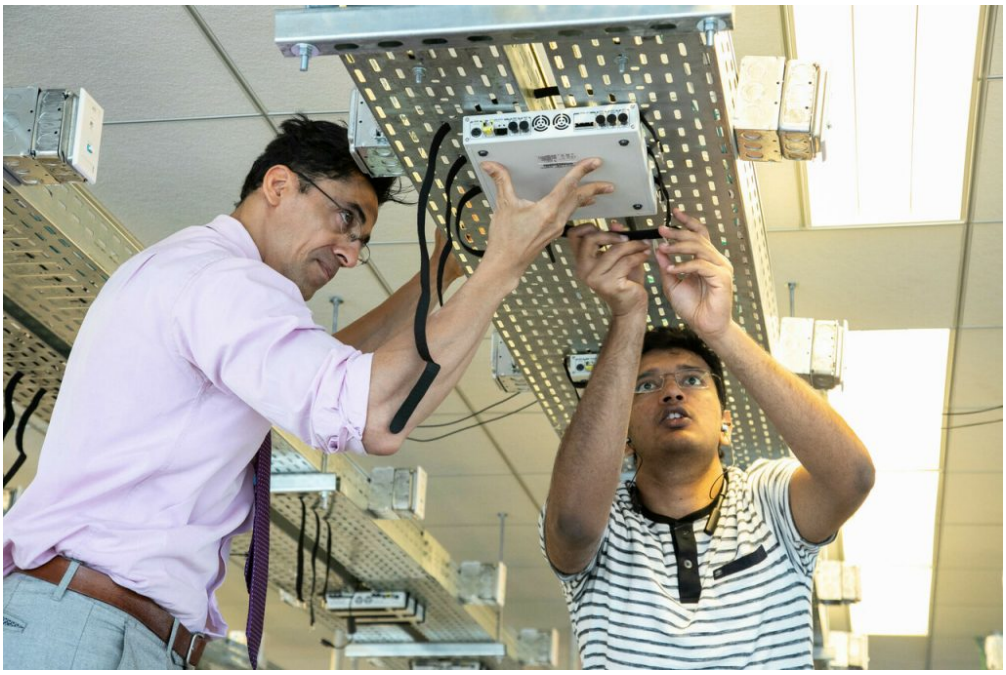


Figure 1.6: CCI xG Testbed Director Aloizio P. DaSilva (at left) installs 72 radio nodes in the Commonwealth Cyber Initiative test bed in Arlington with help from graduate student Vikas Radhakrishnan. The test bed was named one of 15 O-RAN testing and integration centers in the world and the only one in the greater Washington, D.C., metro area. Photo by Anthony Wright for Virginia Tech.

Figure 1.7: New facilities at ODU house the CCI CoVA Node and the School of Cybersecurity.

- 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 inaugural TAB. Its members are (Figure 1.11):

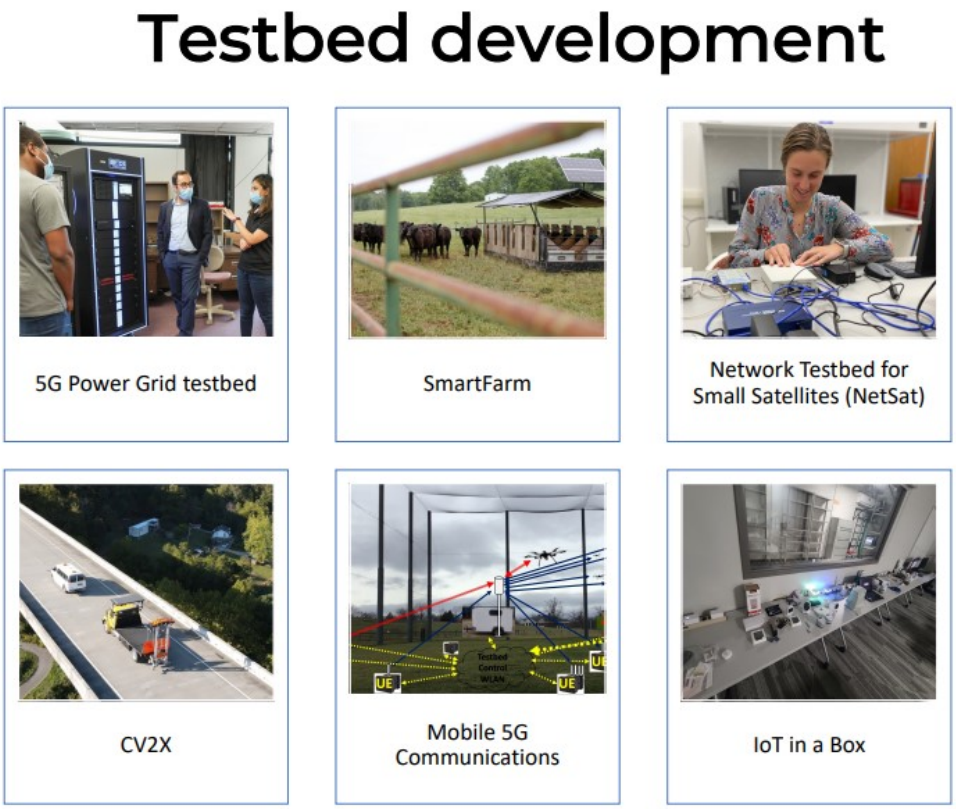


Figure 1.8: SWVA Node snapshot of infrastructure upgrades for FY23.

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

The full TAB meets once a year. FY23's meeting, held on August 31, 2022, was the first held in hybrid mode, with TAB members participating in person as well as remotely. The agenda included a briefing on the State of CCI by the Executive Director, a presentation on CCI's Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT) program by the NoVA Node Director, a briefing on workforce development and innovation programs by the CCI Director of Workforce Development and Innovation, and a discussion of research funding opportunities. Time was also set aside by open discussion and advice from the TAB.

The TAB also formed a sub-committee to select the winner of the CCI Impact Award 2023. 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 Gisele Stolz, a staff member from Mason.

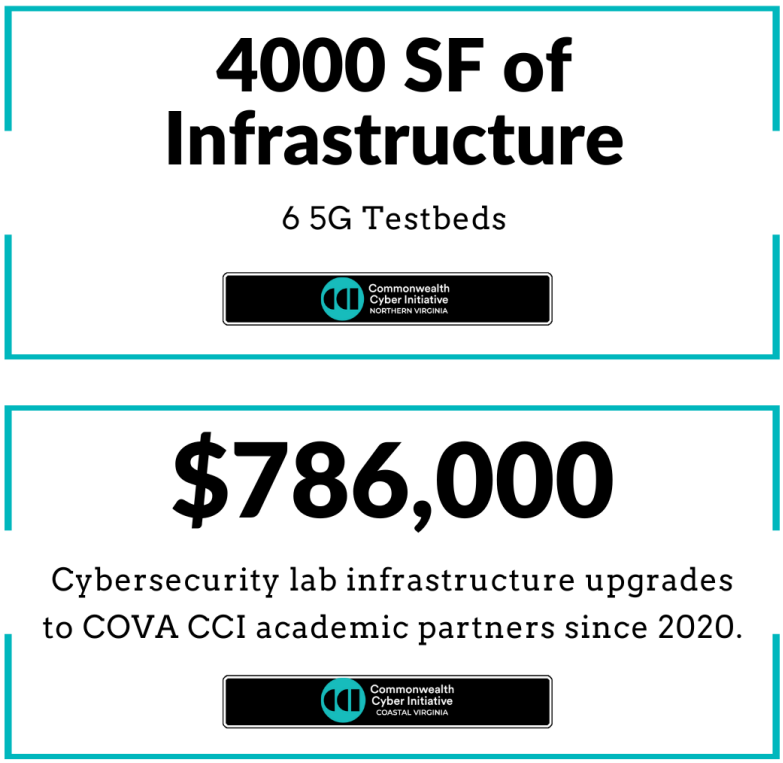


Figure 1.9: A snapshot of NoVA Node infrastructure and CoVA Node infrastructure spending.

Figure 1.10: The CVN Medical Device Security Testbed at VCU.

In Fiscal Year 2024 (FY24) we are planning the first fully in-person meeting of the TAB, to be held in the CCI Hub's facilities in Arlington.

(a) Prof. Elisa Bertino.

(b) Mr. David Ihrie.

(c) Prof. Melur (Ram) Ramasubramanian.

(d) Prof. Sennur Ulukus.

(e) Ms. Tracy Gregorio.

(f) Mr. Jim Mollenkopf.

(g) Mr. Zachary Tudor.

(h) Mr. Dan Woolley.

Figure 1.11: CCI Technical Advisory Board (TAB).

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 Artificial Intelligence (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). The committee is in the process of updating its membership. Additional members are:

- Ms. Jeniffer Allen, CCI program coordinator, CVN;
- Mr. Jordan Mason, CCI program manager, NoVA;

- Ms. Michele McDonald, CCI director of communications and marketing;

In FY23, the CCI Inclusion and Diversity Committee hosted a fall workshop entitled Drawing A Diverse Applicant Pool, featuring Mr. Jordan Mason, who offered advice on strategies CCI Regional Nodes could use to increase diversity among program applicants.

The committee also hosted a Tech Talk on Bias in AI at the 2023 CCI Symposium. Laura Freeman, director of the Intelligent Systems Lab in the Hume Center for National Security and Technology, and Ben Harvey, CEO and founder of AI Squared, discussed how data and societal bias are impacting trust and acceptance of AI research, algorithms, and assumptions.

In addition, the committee recommended that CCI Calls for Proposals feature inclusion language such as "women, underrepresented minorities, and persons with disabilities are strongly encouraged to apply." CCI has applied this recommendation to its calls for proposals and other programs.

1.5 CCI Communications

1.5.1 CCI Social Media Strategy, Website, and Metrics

The CCI Communications and Marketing Team is delivering a consistent and cohesive message to enhance CCI's name recognition and create awareness for researchers, partners, events, programs, and more.

The website is the foundation of our communications strategy. Social media posts, email campaigns, and our popular newsletter are designed to drive people to the CCI website to learn more. Traffic in FY23 increased to 36,535 users, a 20.3 percent jump from FY22.

We have expanded coverage and fine-tuned the layout. Standout web pages include redesigned Call for Proposals and the new Research Showcase. We're also building out the Innovation, Workforce Development, Diversity and Researcher Directory pages. In addition, micro-sites for the xG Testbed and topic-specific projects efficiently convey needed information to our stakeholders.

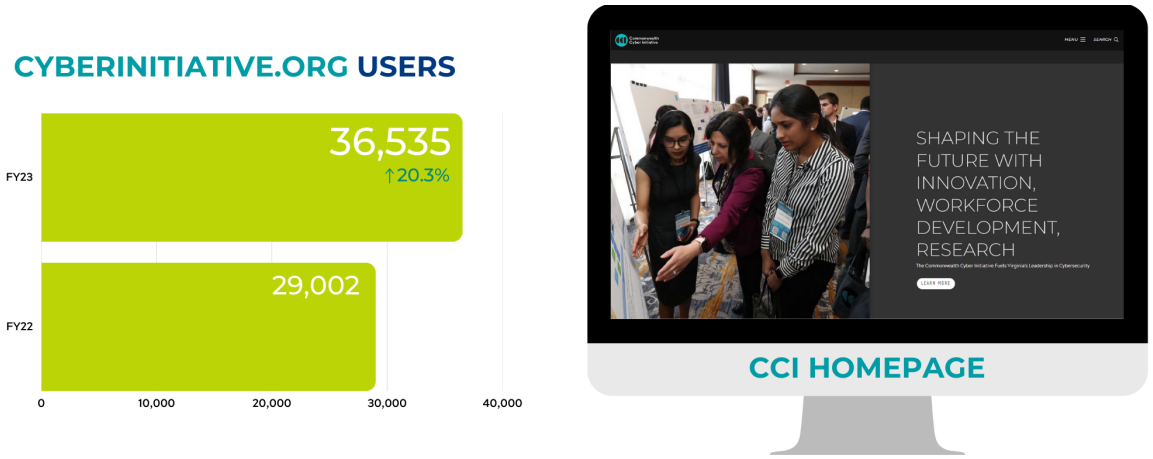


Figure 1.12: Evolution of website usage, focusing on users and page views from July 2022 to June 2023.

Our social media accounts continue to attract followers as we add informative videos and other posts to the mix. These posts drive people to our website to learn more.

- Our LinkedIn audience grew to 1,827 followers, a 77.9% increase from FY22.
- Our Twitter account grew 20.8% to 464 followers and posts were seen 41.3% more frequently in FY23 compared with the prior year.
- Our Instagram account now has 163 followers, an increase of 148.5% from FY22.

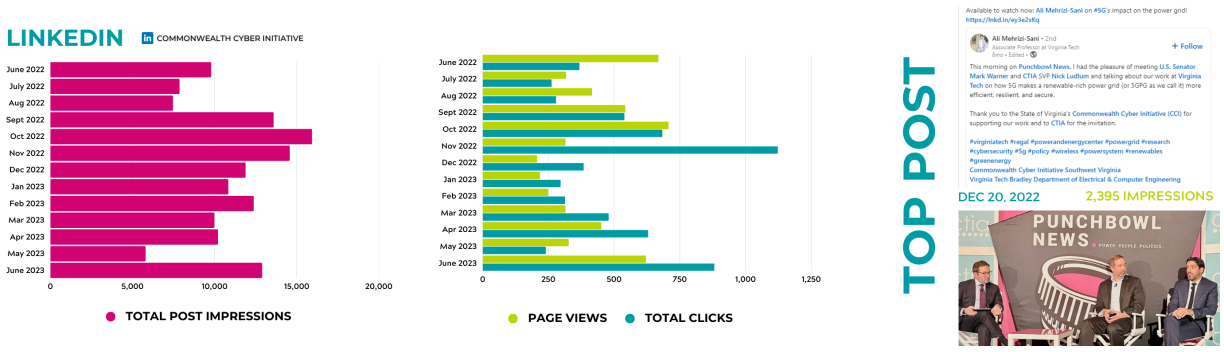


Figure 1.13: Social media followers for CCI's LinkedIn account from July 2022 to June 2023.

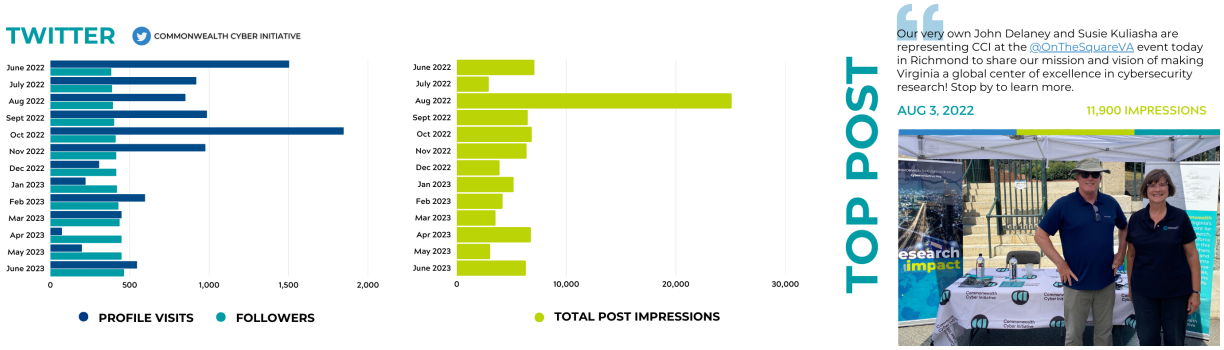


Figure 1.14: CCI Twitter impressions, profile visits, and followers from July 2022 to June 2023. The post with the highest number of impressions is also shown.

Figure 1.13 shows the evolution of our social media followers for LinkedIn, Twitter, YouTube and Instagram, accounts over the past fiscal year.

Our monthly newsletter keeps our highly engaged audience informed while guiding them to the website. Newsletter subscribers have increased to 3,000 from 300 in October 2020.

CCI's visual identity has helped us stand out. Our creative graphics put CCI's refreshed branding to good use, and we're building a cybersecurity-specific photo and video library. We created an About CCI video and a CyberArts Exhibit video in FY23, among several others, and including tech demo videos.

We began producing high-quality, info-packed, and easily skimmable one-pagers during the summer of 2023. Topics include: About CCI, the xG Testbed, the Internship and Job Fair, our Project-Based Learning Program, and more.

The communications team is leading our second CyberArts Program, which funded six projects in FY23, building on the success of the inaugural program in 2020. Projects from the first program were showcased at an art exhibit at the Taubman Museum of Art in Roanoke, Va. Nearly 600 patrons attended the 1.5-day exhibit in November 2022. We are already planning the next exhibit based on the 2023-funded projects.

1.5.2 Appearances in the Media in FY23

Many of the programs and major achievements from CCI researchers and staff have appeared in the print and online media. We posted 193 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 information.

A sampling of media appearances is provided below:

Partnership pushes cybersecurity workforce development to new heights A partnership between CACI International and the Commonwealth Cyber Initiative is building a skilled cyber workforce for the more than 60,000 open cybersecurity jobs in Virginia. "By partnering with industry leader CACI, CCI researchers and students are able to work on real-world problems," said Luiz DaSilva, CCI executive director. Mission line:

Workforce Development

Students Inducted into Cyber LeADERS Program The Cyber LeADERS scholarship program provides up to three years of support, including a full in-state tuition scholarship, an annual stipend ranging from $25,000 (undergraduates) to 34,000 (graduate students) and a professional development allowance. The project prepares students from Tidewater Community College, Virginia Peninsula Community College, and Old Dominion University for federal careers. Mission line: Workforce Development

Study shows impact of cybercrime on Virginia businesses and residents "Cybercrime in Virginia: Impacts on Industry and Citizens." funded by the Coastal Virginia Center for Cyber Innovation (COVA CCI), surveyed more than 420 businesses and 1,200 residents. Eighty-five percent of businesses and 62 percent of residents reported being victimized by a cybercrime. The study was conducted by Old Dominion University, Virginia Commonwealth University, and Virginia Tech. Mission line: Research

Radford University's cybersecurity program awarded global accreditation Radford's School of Computing and Information Sciences degree program in cybersecurity has achieved accreditation by ABET, the global accreditor of college and university programs in computing, engineering and engineering technology. ABET accreditation indicates programs produce graduates ready to enter critical technical fields in innovation and emerging technologies. Mission line: Workforce Development

Virginia State University Computer Science Program Named National Center of Excellence in Cyber Defense The National Security Agency designated VSU, a National Center of Academic Excellence in Cyber Defense (CAE-CD). This recognition goes to academic institutions that have demonstrated exceptional education and research capabilities in cyber defense. Mission line: Research, Workforce Development

CCI's Norfolk State, UVA among universities to train AI to outmaneuver cyber threats A group of universities that includes Norfolk State and UVA is using millions in National Science Foundation (NSF) funding to research how artificial intelligence (AI) might detect and respond to cybersecurity breaches. The program is part of the NSF's AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION). Mission lines: Innovation, Research

Amazon partners with Mason and NVCC for workforce development Students from George Mason University and Northern Virginia Community College participated in the AmazonNext x CodePath, a 10-week course in which they completed CodePath Org's Technical Interview Prep, engaging with real-world software topics and practicing technical interviewing. Mission line: Workforce Development

Virginia governor, NOVA, Google announce cybersecurity training program Governor Glenn Youngkin joined Google executives to announce a new Google Career Certificate in Cybersecurity at Northern Virginia Community College. Built by cybersecurity experts at Google, the certificate will help businesses fill critical roles and enable more job seekers to access well-paying cybersecurity jobs. Mission line: Workforce Development

VCU researchers fight cybercrime with new digital forensic tools and techniques Irfan Ahmed, associate professor of computer science, is leading a pair of interrelated projects funded by the Department of Homeland Security aimed at ensuring the safety of important industrial systems such as nuclear plants, dams and other critical infrastructure. Mission lines: Research, Innovation

Computer science researchers lead defense against the dark side of tech Assistant Professor Bimal Viswanath and his colleagues at Virginia Tech have amassed one of the largest datasets of AI-manipulated media in existence to detect and disarm weaponized media and toxic misinformation campaigns. Mission line: Research

Virginia Senators Warner, Kaine visit future site of Germanna Community College Cybersecurity Training Center Germanna's new Cybersecurity Training Center will house cybersecurity degree and credential programs. Meeting the needs of the cybersecurity workforce is one of the country's biggest challenges, Warner said. "There are 3 million unfilled cyber jobs — 60,000 of them in Virginia." Mission line: Workforce Development

Amazon, Mason Collaborate on Innovations Powered by the Cloud A multi-year initiative between Amazon and George Mason will enable the university to accelerate innovations in workforce development, and national defense R&D. Mission lines: Research, Workforce Development

Virginia Tech-Germanna Community College partnership to increase access to cybersecurity education An agreement between Virginia Tech and Germanna Community College will help increase access to world-class cybersecurity education in the greater Washington, D.C., metro area. The initiative will provide a guided transfer path for Germanna students toward a bachelor's degree in cybersecurity management and

analytics. Mission line: Workforce Development

Mason gets funding for Center for Excellence in Government Cybersecurity Risk Management and Resilience Mason will receive federal funding to support a first-of-its-kind Center for Excellence in Government Cybersecurity Risk Management and Resilience. The center will enhance government cybersecurity and IT modernization efforts, translate state-of-the-art research on technology and cybersecurity in federal practice, and disseminate best practices to agencies. Mission lines: Innovation, Research

Diversifying the quantum workforce Commonwealth Cyber Initiative researchers are collaborating with historically Black colleges and universities to train faculty members in quantum engineering, acquire new quantum lab equipment, and develop quantum curricula to meet the growing demand for a cybersecurity workforce with quantum training. "This is a unique springboard because it allows students to pursue quantum specialties in almost any field," said Wayne Scales, electrical and computer engineering professor from Virginia Tech. "We're on the way to having three Virginia universities with this unique laboratory infrastructure." Mission line: Workforce Development

CCI researchers recognized

Chen-Ching Liu, Virginia Tech. The electrical and computer engineering professor, and his team will implement new technologies as part of a multi-million dollar Department of Energy grant to improve electrical substation cybersecurity.

Liza Wilson Durant, George Mason University. The director of CCI's Northern Virginia Node was among those recognized with a Virginia Business Women in Leadership Award.

Dmitry Evtyushkin, College of William & Mary. The assistant professor in the Department of Computer Science won a five-year CAREER award from the National Science Foundation for his work in securing computer microarchitecture.

Milos Manic, Virginia Commonwealth University. The professor of computer science in the College of Engineering and director of VCU's Cybersecurity Center has been elected by the National Academy of Inventors to the rank of senior member. The honor goes to those who have produced technologies that have brought, or aspire to bring, real impact on the welfare of society.

Adwait Nadkarni and Oscar Chaparro, College of William & Mary. The assistant professors in the Department of Computer Science won NSF Career Awards for projects focusing on smart device security compliance and software code change decisions.

Thanhvu Nguyen, George Mason University. The assistant professor in the Department of Computer Science won an NSF CAREER Award for his work on technology that ensures AI machine learning is robust, safe, and unbiased.

Danfeng "Daphne" Yao, Virginia Tech. The professor in the Department of Computer Science has been elevated to fellow, the highest grade of membership in the Institute of Electrical and Electronics Engineers (IEEE), for her contributions to enterprise data security and high-precision vulnerability screening.

1.6 Report Structure

This report describes the CCI's progress and achievements in FY23. 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 FY23. Finally, Chapter 7 describes our main activities and programs planned for FY24.

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;

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.

- 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 FY23 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 FY23

In FY23, the CCI network received 111 external grants totaling $75,142,580 to support the CCI mission lines of research, workforce development and innovation. 78 grants (70%) were from federal agencies and 33 grants (30%) were from state and industry. 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 FY23, 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 Securing Interactions between Humans and Machines

Objective of the Call

One of the research themes selected by CCI is securing the interactions between humans and machines. It is the focus of this call for proposals.

Recent evolution in artificial intelligence, cyber physical systems, and communications are leading to a world in which humans and autonomous machines increasingly interact. In CCI, we view cybersecurity as intrinsically cross-disciplinary and devise solutions that lead to secure, resilient, and harmonious interactions between people and robots, drones, autonomous vehicles, and other cyber physical systems.

Our research focuses on the technological challenges in securing this enhanced digital world experience, in close collaboration with experts from the social sciences, life sciences, health sciences, public policy, law,

CCI Extramural Funding for FY23

Federal Grants	State/Industry Grants
78	33
$69,188,082	$5,954,498

CCI Extramural Funding for 2023 by Node

Node	Number of Grants	Grant Total
CCI Hub	9	$977,811
Central Virginia	8	$8,161,000
Coastal Virginia	22	$6,366,960
Northern Virginia	36	$43,676,883
Southwest Virginia	36	$15,959,926
Total	**111**	**$75,142,580**

Figure 2.1: External funding obtained by the CCI network in FY23.

and humanities. Topics of interest include, but are not limited to: artificial intelligence assurance; securing the metaverse; security and privacy for embedded and/or wearable devices; the role of human behavior in securing the digital world; and ethical cybersecurity.

Objectives of this call include:

- To produce seminal contributions to securing the interactions between humans and machines, targeting the expansion of this research through competitive grants from the federal government, private sector, philanthropic foundations, and other sources.
- To contribute to workforce development in cybersecurity with cross-disciplinary domain knowledge.
- To explore opportunities for innovation (commercialization, entrepreneurship, etc.) in security and privacy for the interaction between humans and machines.

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 (securing the interactions between humans and machines) and strong rationale for a cross-disciplinary approach.
- 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.

Research Grants Awarded

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.

Securing Interactions between Humans and Machines Research Program

Node	Number of Grants	Grant Total
Central Virginia	3	$180,000
Coastal Virginia	2	$120,000
Northern Virginia	1	$60,000
Southwest Virginia	2	$120,000
Total	**8**	**$480,000**

Figure 2.2: Securing interactions between human and machines research program details for FY23.

2.2.2 SWVA 2023 Research Engagement Program

Objective of the Call

The Cybersecurity Research Engagement Program exists to seed research efforts along two tracks:

- Track 1: Large-scale proposal development - Seed funds for pilot studies, dedicated research time, collaboration, or other support to increase proposal competitiveness. External funding program, amount, anticipated team, and submission date must be specified in the proposal. Single-institution teams are welcome.
- Track 2: Startup engagement - Funds to engage students or faculty with startups. The company must have operations in Virginia and must be specified in the proposal.

  Focus areas should be related to the intersection of data, autonomy, and security. CCI Southwest Virginia has a particular emphasis on cybersecurity-related to fast, secure, and customizable communications systems and technologies, including 5G, artificial intelligence (AI), machine learning (ML), defense-in-depth cybersecurity solutions, emerging technologies (such as NextG and quantum algorithms) and cryptographic protocols, applications in transportation, energy, space, autonomous systems, manufacturing, and agriculture, as well as issues surrounding human factors, privacy, ethics, and global security in society.

Selection Criteria

Proposals were reviewed by subject matter experts and evaluated according to the following criteria:

- Intellectual merit (40%): clearly defined problem/unmet need and how proposed work will address it.
- Broader impact (10%): potential to benefit society and contribute to the achievement of specific, desired societal outcomes, as it aligns with CCI's mission..
- Value of the funding (20%): concrete plans to use the results from this research to secure external funding or Intellectual Property (IP).
- Alignment and qualifications (30%): relevance to CCI mission and suitability of team background to proposed work.

Research Grants Awarded

The peer review process resulted in 13 research grants awarded, as shown in Appendix 1.

2.2.3 CCI Fellows Program 2023

This program, launched in Fiscal Year 2022 (FY22) and continued throughout FY23, 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 will fund CCI researchers to lead center-scale proposals. PIs funded under this call will be designated 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 will be 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 FY23 CCI Fellows are listed in Figure 2.3.

CCI 2023 Fellows

Fellow	University
Dr. Aidong Zhang	University of Virginia
Dr. Jack Davidson	University of Virginia
Dr. Jonathan Black	Virginia Tech
Dr. Jonathan Goodall	University of Virginia
Dr. Mohamed Azab	Virginia Military Institute
Dr. Parth Pathak	George Mason University

Figure 2.3: CCI Fellows FY23.

2.2.4 CCI CyberArts Program

Objective of the Call

The CyberArts program challenges the Arts and Design research community to reimagine and depict the results of cybersecurity research (in particular, research that occurs in CCI) for either scientific or creative arts purposes. We encourage transdisciplinary partnerships with CCI researchers, but will give priority to proposals led by researchers in the Arts and Design disciplines.

The program is funded by CCI and co-organized with the Institute for Creativity, Arts, and Technology at Virginia Tech, and the da Vinci Center for Innovation at Virginia Commonwealth University.

CCI held an exhibit of the 2020 CyberArts funded projects in November of 2022 at the Taubman Museum of Art in Roanoke, Va., and is planning for a museum exhibit for the 2023 funded program.

Selection Criteria

A review committee reviewed the proposals and made funding recommendations. Evaluation criteria include:

- Strong intellectual merit related to cybersecurity and the arts.
- Relevance to the focus of the call (intersection between cybersecurity and Arts and Design).
- Strong broader impacts related to CCI's mission lines of innovation, research, and workforce development.
- Tangible outcome from the project, such as a piece of art or performance.

2023 Cyber Arts & Design Research Program

Node	Number of Grants	Grant Total
Central Virginia	1	$25,000
Coastal Virginia	1	$25,000
Northern Virginia	2	$50,000
Southwest Virginia	2	$50,000
Total	**8**	**$150,000**

Figure 2.4: Cyber Arts and Design FY23 research program award details.

Research Grants Awarded

The peer review process resulted in six grants awarded, as summarized in Figure 2.4.

2.3 Faculty Recruited

2.3.1 Hub Faculty

The CCI Hub hired two new research faculty members, one post-doctoral researcher, and had two researcher promotions in FY23. They are:

Dr. Eric Burger is the CCI Research Director. His primary appointment at CCI is Research Professor of NextG Security, with courtesy appointments as Research Professor of ECE and Research Professor of Public Policy at VT. He is also affiliated with Wireless@VT, the National Security Institute, and the Department of Computer Science. He currently also serves as the Technical Program Director of the Next G Alliance. Dr. Burger served as the Assistant Director for Telecommunications and Cybersecurity of the White House Office of Science and Technology Policy and as the Chief Technology Officer of the Federal Communications Commission. Prior to Virginia Tech, Dr. Burger was Research Professor of Computer Science at Georgetown University, where he was founding director of the Georgetown site of the NSF Security and Software Engineering Research Center and Cyber SMART IUCRC. Prior to academia, Dr. Burger started or turned around several network equipment companies, serving as CTO and SVP Engineering, from venture-backed startups to large private equity, NASD-listed, and NYSE-listed companies. He has a SBEE, MBA, and PhD from the Massachusetts Institute of Technology, Katholieke Universiteit te Leuven, and Illinois Institute of Technology. Dr. Burger is a Life Distinguished Member of the ACM, a Senior Member of the IEEE, a Senior Member of the National Academy of Inventors, and a Life Member of AFCEA.

Dr. Shin'ichiro Matsuo is a CCI Research Professor at CCI and VT though hired in FY23, Dr. Matsuo's start date is FY24. His research focuses on applied cryptography, security, privacy protection, and

blockchain technology. He is also a Research Professor of Computer Science at Georgetown University. He received his PhD in 2003 from Tokyo Institute of Technology. He has published over 80 papers on fundamental cryptography and cryptographic protocols. Dr. Matsuo served as a Technical Program Committee (TPC) chair for IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2022, Workshop on Coordination of Decentralized Finance (CoDeFi) 2020-2023, Scaling Bitcoin 2018, Security Standardization Research 2015, as well as a member of the editorial committee of IEEE Transactions on Dependable and Secure Computing (TDSC), and as a steering committee member of Security Standardization Research from 2014 to present. He also served as a project editor of six ISO/IEC standards and reports. Dr. Matsuo is an acting co-chair of the Blockchain Governance Initiative Network (BGIN), and a member of the OECD Blockchain Expert Policy Advisory Board (BEPAB).

Dr. Priyanka Sinha is the CCI and VT Presidential Postdoctoral Associate. She received her BS in Electrical Engineering from the National Institute of Technology, Durgapur, India, her MS in Electrical and Computer Engineering from the University of Florida, and her PhD in Electrical Engineering along with a minor in the Department of Mathematics at North Carolina State University. Dr. Sinha's research interests, include: adversarial learning, auction learning, security and privacy in machine learning, optimization, functional analysis, and cybersecurity of wireless communication systems. Between the years of 2013 - 2018, she worked as a Systems Engineer at Qualcomm, Inc.

Dr. Jacek Kibilda was promoted to Research Associate Professor for CCI and VT in the Bradley Department of Electrical and Computer Engineering. He is a contributing member of the ATIS Next G Alliance Spectrum working group and is a Fulbright Fellow. Dr. Kibilda's research, that is sponsored by federal and industry funding, focuses on advanced mobile architectures toward flexible, reliable, and secure Next G networks.

Dr. Joao Santos was promoted to Research Assistant Professor with CCI and VT. He was nominated and inducted into Virginia Tech's Edward A. Bouchet Graduate Honor Society, is an IEEE member, and serves as a member of Virginia Tech's Center for the Integration of Research, Teaching, and Learning (CIRTL) Advisory Board. Dr. Santos' main research interests include open radio access networks, radio virtualization, network slicing, and network orchestration.

2.3.2 Node Faculty

2.3.3 Northern Virginia Node

Dr. Zhengdao Wang Dr. Zhengdao Wang 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, in partnership with researchers from the Coastal Node of the Commonwealth Cyber Initiative and Old Dominion University. He and his counterpart at ODU will have access to the faculty and facilities of both George Mason University and Old Dominion University to enable their success.

Dr. Wang received his Bachelor's degree in Electronic Engineering and Information Science from the University of Science and Technology in China (USTC), M.S. degree in Electrical Engineering from the University of Virginia, and Ph.D. degree in Electrical and Computer Engineering from the University of Minnesota. Since 2002, he has served on the faculty of the Department of Electrical and Computer Engineering at Iowa State University. He held a visiting professorship from UTSC from 2012-2015. He served as a Program Director at National Science Foundation in the Division of Electrical, Communications, and Cyber Systems from 2020 to 2022. Dr. Wang has served as an editor on numerous IEEE publications including: Transactions on Vehicular Technology, IEEE Signal Processing Letters, IEEE Transactions on Signal Processing, IEEE Transactions on Wireless Communications, and IEEE Signal Processing Society Online Video Library. He has received numerous awards and recognitions and is an IEEE Fellow since 2016. His interests are in the areas of machine learning, cybersecurity, communications, signal processing, and information theory.

Dr. Xin-Wen Wu CCI NoVa Node provided continued support to University of Mary Washington and Dr. Xin-Wen Wu. Dr. Wu's research interests include networked systems security, security protocols for the Internet of Things (IoT) and cloud computing, applied cryptography and 3D encryption, applications of machine learning to cybersecurity, and cybersecurity education. He has published 3 books and over 100

refereed papers in reputable journals (such as IEEE Transactions on Information Forensics and Security) and international conference proceedings. Over the past several years, he has been working on IoT security making use of machine learning technologies. His research project on anomaly detection and risk mitigation enabled by collaborative machine learning was funded by the NSA's NCAE-C Cybersecurity Education Research Innovation program.

Dr. Suk Jin Lee CCI NoVa Node supported the hiring of Dr. Suk Jin Lee by James Madison University. Dr. Lee, who received his Ph.D. in Electrical and Computer Engineering from Virginia Commonwealth University, will join JMU's faculty in Fall 2023. Dr. Lee's interests include cybersecurity, IoT, network protocols, computer vision, machine learning and neural networks, pattern classification, target tracking, and signal processing.

2.3.4 Coastal Virginia Node

Chris Shenefiel Chris Shenefiel is a CCI Senior Cyber Law Researcher at William and Mary. Previously, he worked for Cisco Systems, where he was responsible for selecting, funding and managing cybersecurity research programs at Cisco Systems. He also served as a Data Scientist; uncovering security vulnerability trends and defining ways to improve Cisco's offer security. In his role as an Adjunct Lecturer he continues to teach a graduate and undergraduate course in Applied Cybersecurity for the William and Mary Computer Science Department and guest lecture in the Law School.

Chris has over 30 years of advanced technology experience in engineering, marketing, consulting and general business management with several of the world's largest communications corporations including Motorola, Southwestern Bell, and AT&T Communications in capacities that include software design, user interface design, applied R&D, professional services, project management and product management. He graduated from the University of Illinois with a Masters in Engineering Psychology and recently earned a Franklin Fellowship at William and Mary Law School.

2.3.5 Southwest Virginia Node

Dr. Charles Cao Assistant Professor, Department of Physicis, Virginia Tech. Dr. Charles Cao was recruited from the Institute for Quantum Information and Matter – Caltech (IQIM) where he was a post-doctoral associate. Previously, he was a QuICS Hartree Postdoctoral Fellow in quantum information and computer science from 2019 to 2022 at the Joint Center for Quantum Information and Computer Science (QuICS) at the University of Maryland. His research spans high-energy physics, quantum information theory, and gravity. He is particularly interested in emergent phenomena in complex manybody systems. His current research focuses on an approach to quantum gravity where space-time and Einstein gravity can emerge from quantum manybody systems. He has worked on problems in holography, cosmology, foundations of quantum mechanics, quantum information, and tensor networks. Charles received his doctorate from the California Institute of Technology in 2018.

Dr. Eduardo Camps-Morenois a Presidential Postdoc and Postdoctoral Associate, Department of Mathematics, Virginia Tech. Dr. Eduardo Camps-Moreno received a Ph.D. degree in mathematics from the Instituto Politécnico Nacional, Mexico, in 2023. His research interests include: information theory, coding theory, especially quantum error correction, and commutative algebra. He has been awarded a Swiss Excellence Scholarship from the Swiss Government in 2021 and a Sotero Prieto Prize for the Best Bachelor's Thesis in Mathematics from the Mexican Mathematical Society in 2018.

Dr. Bahman Abolhassani is a Presidential Postdoc and Postdoctoral Associate, Bradley Department of Electrical and Computer Engineering, Virginia Tech. Dr. Bahman Abolhassani received the B.Sc. and M.Sc. degrees in electrical engineering from the Sharif University of Technology (SUT), Tehran, Iran, in 2015 and 2017, respectively. He is received the Ph.D. degree from the Department of Electrical and Computer Engineering, The Ohio State University, in 2023. From 2015 to 2017, he was a Researcher with the Optical Networks Research Laboratory, SUT. His research interests include communication networks, optimization theory, caching, and algorithm design.

Dr. Emily McMillon is a Presidential Postdoc and NSF Postdoc, recruited in FY23 with an FY24 start date.

2.3.6 Central Virginia Node

The Central Virginia Node did not recruit new faculty members in FY23.

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.

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 2.5 shows the logo developed for the testbed.

Figure 2.5: 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 the past two years. These published papers are focused on cybersecurity, have advanced the field, and have benefited from our programs.

CCI will issue periodic calls for papers as we continue to share our researchers' contributions to the world's knowledge on our website and through social media platforms.

P2 O: AI-Driven Framework for Managing and Securing Wastewater Treatment Plants Authors: Ajay Kulkarni; Mehmet Yardimci, Md Nazmul Kabir Sikder, and Feras A. Batarseh Publication/Conference: Journal of Environmental Engineering, American Society of Civil Engineers (ASCE) Publication/Presentation Date: June 2023

Cyber Vulnerability Assessment of Microgrids with 5G-Enabled Distributed Control Authors: Ardavan Mohammadhassani, Yousef Akbar, Ali Mehrizi-Sani, and Haining Wang Publication/Conference: 2022 IEEE Power and Energy Society General Meeting (PESGM) Publication/Presentation Date: July 2022

MANDA: On Adversarial Example Detection for Network Intrusion Detection System Authors: Ning Wang, Yimin Chen, Yang Xiao, Yang Hu, Wenjing Lou, and Y. Thomas Hou Publication/Conference: IEEE Transactions on Dependable and Secure Computing (TDSC), vol. 20, issue 2 Publication/Conference Date: March-April 2023

Scheduled Spatial Sensing against Adversarial WiFi Sensing Authors: Steven M. Hernandez, Eyuphan Bulut Publication/Conference: 21st International Conference on Pervasive Computing and Communications (PerCom 2023) Publication/Presentation Date: March 13-17, 2023, Atlanta

Cyberattack Correlation and Mitigation for Distribution Systems via Machine Learning Authors: Jennifer Appiah-Kubi, Chen-Ching Liu Publication/Conference: IEEE Open Access Journal of Power and Energy, Vol. 10 Publication/Presentation Date: January 12, 2023

Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage Authors: Sunil Manandhar, Kaushal Kafle, Benjamin Andow, Kapil Singh, Adwait Nadkarni Publications/Conference: Proceedings of the 31st USENIX Security Symposium (USENIX) Date of Publication/Presentation: August 2022

Strategic Safety-Critical Attacks Against an Advanced Driver Assistance System Authors: Xugui Zhou; Anna Schmedding; Haotian Ren; Lishan Yang; Philip Schowitz; Evgenia Smirni; Homa

Alemzadeh Publication/Conference: 2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) Publication/Presentation Date: July 25, 2022

Spatiotemporal G-Code Modeling for Secure FDM-based 3D Printing Authors: Muhammad Haris Rais, Ye Li, Irfan Ahmed Publication/Conference: 12th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS) Publication/Presentation Date: May 2021

Understanding IoT Security from a Market-Scale Perspective Authors: Xin Jin, Sunil Manandhar, Kaushal Kafle, Zhiqiang Lin, Adwait Nadkarni Publication/Conference: Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS) Date of Publication/Presentation: November 2022

Hybrid Knowledge and Data Driven Synthesis of Runtime Monitors for Cyber-Physical Systems Authors: Xugui Zhou; Bulbul Ahmed; James H. Aylor; Philip Asare; Homa Alemzadeh Publication/Conference: IEEE Transactions on Dependable and Secure Computing Publication/Presentation Date: February 2023

2.5.1 Highlight: Securing the Power Grid

CCI researchers have been particularly impactful on scholarship and funding around the topic of securing the power grid. CCI has invested in a 5G for the Power Grid (5GPG) testbed, which our researchers are leveraging to:

- secure power grid communication systems for military base installations and the Virginia Tech Blacksburg campus;
- launch the Virginia Power Analytics and Cybersecurity (VPAC) Service Center, which is accelerating cyber technology commercializing by providing companies with a service to evaluate new technologies before they are deployed in the power system;
- grow cyber training opportunities through Real-Time Simulation of the Power System Training Workshop for students.

The 5GPG testbed started as a digital twin of the Virginia Tech Electric Service system, which enabled real-time co-simulation of hardware-in-the-loop power systems and communication networks to anticipate possible cyberattacks among other goals. In the last year, 5GPG researchers are expanding beyond Blacksburg and applying the models and methods to secure future U.S. military bases and their critical missions from cyberattack.

Researchers involved with this project are investigating how 5G and NextG wireless networks can provide wider network coverage and faster data transmission to support a secure smart grid that integrates distributed energy resources.

In alignment with CCI's commitment to accelerate cyber startup creation and technology commercialization, the 5GPG research team recently launched the VPAC Service Center. This center provides services to outside entities (utilities, consulting firms, other universities), including Real Time Digital Simulator (RTDS) of the Power System. RTDS is a major component of the 5G power grid testbed and is an industry standard tool to evaluate new technologies before they are deployed in the power system. The current RTDS setup was purchased through CCI funds as well as a donation from Dominion Energy.

In addition, the 5GPG team has been growing cyber training by offering an RTDS Training Workshop to students in connection with the VPAC Service Center. Students now have the opportunity to receive training in RTDS operation — a highly sought-after skill in the power industry. Plans are underway to expand the setup in the coming years.

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 section 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 over two days in late September and proves again to be one of our most popular programs. Over 500 students registered for this free and virtual event comprising career panels and employer booths. Twenty-one employers participated ranging from government agencies to small Virginia-based companies. Featured employers included: CACI, Microsoft, G2Ops, and Health and Human Services.

3.1.2 CyberFusion

The Commonwealth Cyber Fusion, hosted by VMI, Senator Mark R. Warner, the Virginia Cyber Range, and CCI took place on the VMI campus on February 24-25, 2023. 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 competed over the weekend, from 20 teams. The team from Tidewater Community College and the team from University of Virginia won their respective divisions. The competition was completely free for student teams and their coaches due to corporate sponsorship and CCI. This enabled all interested teams to compete, regardless of fundraising ability.

3.1.3 Project-based Learning Program

Project-based learning is a pedagogical shift in academia, whereby students are actively engaged in a sponsored project while learning in the classroom. It allows students to actively apply learning principles, solidify those learning principles, and gain meaningful experiences in the process. 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 is with CACI and Northern Virginia Community College (NVCC). CACI has accepted seven cyber students from NVCC who will work on two discrete projects for two semesters. CCI will pay the students' stipend and monitor the projects. This program has already earned much interest from industry partners and community colleges across the state and we look forward to scaling this program in FY24.

3.1.4 Clearance Preparedness Program

In FY23 the CCI Hub began a virtual series to prepare students for the security clearance process, scaling existing programs from the regional to the state level. 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 certificate 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 FY23

In its fourth iteration, the 2023 Experiential Learning call for proposals elicited 28 submissions, with seven successful proposals totalling $699,370 awarded in grants. CCI researchers were eligible to respond to this call, and proposals were selected based on recommendations by a peer review group. The percentage of the funding for projects in each CCI Node is shown in Figure 3.1.

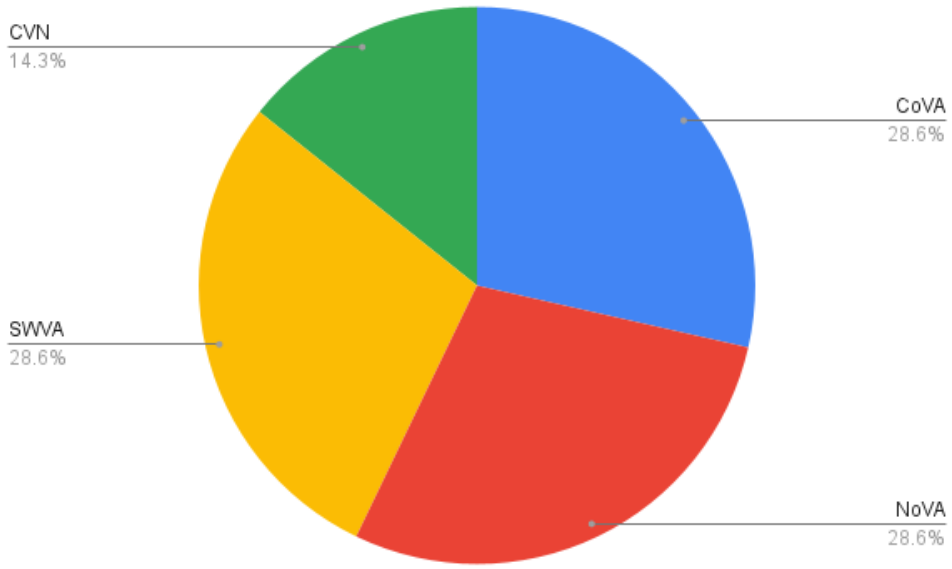


Figure 3.1: Funding percentage by Node for the FY23 Experiential Learning program.

The projects funded by this program are summarized below.

- **From Experiential Learning to Practice: A Pre-Apprenticeship Program**: Stephanie J. Blackmon; William & Mary (W&M); $89,370. In the curricular phase, subject matter experts (SMEs) will work with students, informing them about the particulars of a job and discussing the process of thinking like a cybersecurity expert. During the application phase, the SME will guide the student, who will have more independent tasks in an internship. The project placement site is Peregrine Technical Solutions, which has a Top-Secret Facility Clearance Level. From November 2023 through April 2024, 16 students will spend 10 hours a week working with SMEs in: Information technology cybersecurity; Internet of Things (IoT) cybersecurity; Operations; Technical Writing. For the next phase (February 2024-April 2024), students will apply that content alongside SMEs while working on unclassified tasks for the federal government. The entire program will be virtual.
- **Cyber Startups**: Gisele Stoltz; George Mason University (Mason); $100,000. The semester-long program will be offered twice a year, in the Spring and Fall, placing 42 Mason students and eight

UMW students into internships. The opportunity will be advertised through relevant Cybersecurity, Computer Science, Information Technology, and other departments, as well as with career services. Applicants will be pre-screened, then presented to employers based on company requirements. Startup companies interview candidates and select their interns, who are then put on Mason's payroll for $19 an hour. Students work up to 125 hours during the internship and are expected to complete projects defined by the host startup. The program manager and the PI hold regular check-ins with interns and the hosts to ensure the internships are going well, projects are progressing in a timely manner, and any issues can be quickly remedied.

- **CyberMobile: Secure Mobile (iOS) Development through Experiential Learning** : Eyuphan Bulut; VCU; $100,000. The two-stage program will train 10 VCU and VUU students in the fundamentals of mobile iOS app programming and security-related practices in the classroom and through industry collaborators. Phase One, Fall 2023: Students will get hands-on studies in VCU's iMAC Lab. Exercises and assignments will involve code training and focus on security vulnerabilities. Phase Two, Spring 2024: Students will hold internships in which they collaborate with employees of industry partners and encounter real-life problems.

- **Solving the Cyber Workforce and Skills Challenges through Experiential Learning**: Brian Ngac; Mason; $100,000. The instructor will work with industry participants to define the project scope, deliverables, expectations, and goals of the experiential learning effort. In 12-week sessions held in an agile environment, students meet clients (industry participants) weekly to present progress, receive feedback, and discuss next steps. Students are instructed to dedicate additional group time (outside of client and instructor meetings) every week for project execution. Students will present their work and discuss lessons learned to interested parties. The instructional team will look for areas to improve and grow the experiential learning effort. Students, who'll be paid a stipend for their work, will also participate in a networking event with industry participants and other select cyber executives.

- **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. VSGC will produce 14 program sessions using test preparation questions. The asynchronous videos will be modeled after the Security+ resource developed under a previous CCI award. A student audience will be used during live session taping using the ZOOM platform. Students will be offered the test preparation manual in appreciation for their role. Closed captioning and transcripts will be featured, and the series will be available through a link on the VSGC website. Student use of the video resources will be tracked through the registration process.

- **Use and Abuse of Personal Information**: Alan Michaels; VT; $100,000. Researchers will extend the original small-scale experiment from a manually constructed set of 300 identities to a more comprehensive automated set of 100,000 fake identities to be shared with second parties in one-time online transactions. Fake IDs are sculpted and assigned to a variety of research questions before performing one-time online transactions. Results of those interactions are aggregated by an enterprise-scale open-source collection engine designed and built by students. This engine transforms incoming emails, SMS texts, and voicemails into labeled datasets to support analysis and comparison of PI sharing behaviors and cybersecurity characteristics of the online transaction (passwords, spam, malware). Of particular interest are cross-site sharing behaviors (attributable due to one-time interactions) and root sources of spam/malicious content.

- **Enhancing Experiential Learning via Technology Enabled Internships with Mentoring (TEIM)**; Jeff Pittges; Radford; $100,000. The TEIM program will ask experienced higher education students to serve as mentors for less experienced college and high school students. The student-mentors will get "mentoring-the-mentor" support from professionals. Once the student-mentor is assigned, the mentee takes the lead to: Work with the student-mentor to establish a routine meeting time; Study curated weekly topic-specific learning materials (written, video, and interactive) in preparation of the meeting; Lead weekly meetings using a provided structured agenda with built-in feedback points;

Capture meeting feedback and data in the Your Career Counselor platform; Perform follow-up actions that include meeting recaps to the student-mentor.

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 node totaled $1,318,943.00 in FY23.

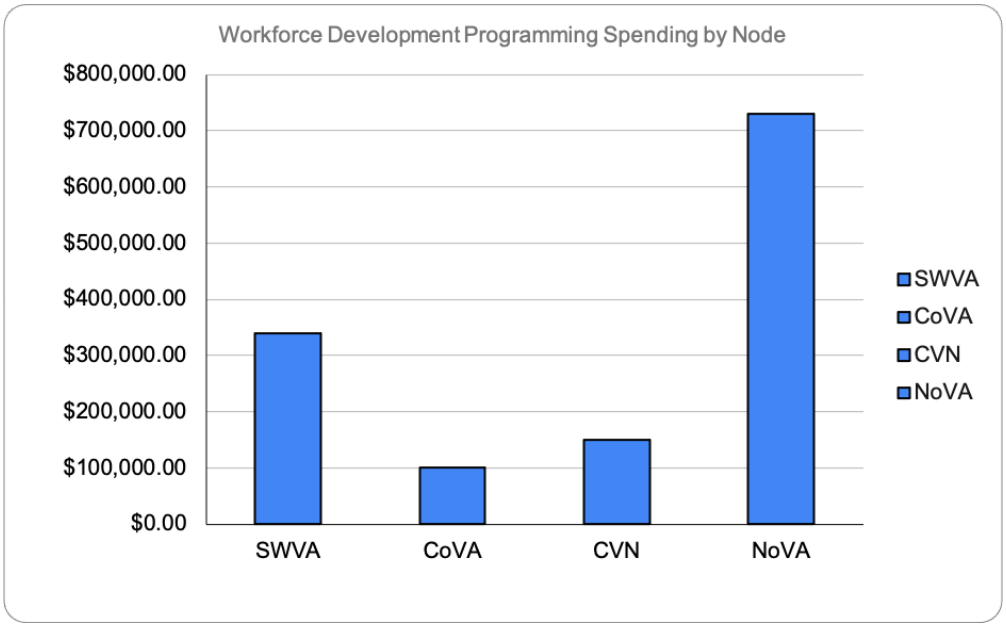


Figure 3.2: Workforce Development spending by Node in FY23.

3.2.1 NoVA Node

The NoVA Node carried out six workforce initiatives:

- **High School Cybersecurity Internship Program**: The CCI NoVA Node is funding 38 high school students for internships with cybersecurity companies during Summer 2023. The experience includes a 2-week professional skills training program to prepare students for the professional work environment. 103 applications were received for the 38 available placements. Of the selected applicants, 41 percent identify as women or non-binary. Host companies include: Appian, Shift5, Virginia Tech Thinkabit Physical Computing Lab, Chainbridge Solutions, CACI, Leidos, NT Concepts, Obscurity Labs, Oceus Networks, 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 2022 and spring 2023. In fall 2022, the program received 290 applications for 28 internships with 14 companies. In spring 2023, 141 applications were received for 23 internships with 11 companies. Thirty-one percent (31%) of the interns were female and 77% identified as minorities. 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, and Pistevo Decision. 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.

Additionally, four of these student interns have launched their own startups. These include Xenophon Analytics and DigiMicro. Two additional students went through the ICAP program, which provides training, mentorship, and wraparound services to entrepreneurs, and have not yet formed their startup.

- **Undergraduate Research Program** CCI NoVA CCI NoVa Node sponsored 30 undergraduate students conducting cybersecurity research at George Mason University, James Madison University and University of Mary Washington. Example research projects included:
  - Security Assessment
  - Energy-Preserving Cryptography for Power Constrained Device
  - Broadband Adoption Rise in Rural Communities Using Rail Tracks
  - Impact of Human Behavior on Hybrid Driving Environment
  - SAWBRID: SmArt WhiteBoard Replacement Interactive Device
  - Healthcare Organizations and their Reliance on Vendors/Cloud Systems
  - Securing the Internet of Things with Artificial Intelligence Technologies
  - Securing the Metaverse: A Privacy-preserving Zero Trust Approach
  - Smart Building Control using NextG Mobile Edge Servers (MEC)
  - The Cyber Workforce Gap's Impact on Organizations
  - Exploring How Convergence Methods Foster Shared Accountability to Reveal, Map, and Mitigate the Sources and Dynamics of Bias across Social Service Provisioning Systems
  - Secure 5G-based Indoor Positioning of Firefighters Using UAVs

  These experiences are building significant technical expertise and capacity in undergraduates, making them particularly well trained for advanced work in industry and government. Forty percent (40%) of this year's Undergraduate Research Assistants cohort identify as women, and 57% identify with underrepresented population groups in science and engineering.

- **Teacher Cybersecurity Professional Development Program**. Twenty-two 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 feedback from last year's participants, CCI NoVa Node and Cyber.org split this year's program into two separate cohorts, one for k-8 and one for 9-12. This shift allowed the program to better meet the needs of teachers serving different student populations. Sessions were 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 2200 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 9, 2023, followed by a 12-week apprenticeship/traineeship with a cybersecurity company. The program received over 105 applications for 20 available positions. 40% of the cohort identify as female. Underrepresented population groups in science and engineering comprise 85% of this cohort. Placement in apprenticeships is ongoing and includes, to date, apprenticeships with InterSec, NetworkFort, Sedulous, and Peraton.

- **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 23 students participating in this program, with more onboarding. Industry hosts include CACI, Cask Government Services, CGI Federal Services, InterSec, Inc., Fend, Inc., IvySys Technologies, NikSoft, NetworkFort, Neuvik, and RPRC. Forty-three percent (43%) of this cohort identify as female and 52% 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 FY23, CCI NoVa Node provided support to the CyberStart program via CodeVa. 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 saw a total of 3504 students register for CyberStart, with 383 of them earning National CyberStart (NCS) Semifinalist designations (10.9%). Students falling within the geographical boundaries of CCI NoVa Node represented 1523 registered students, with 229 qualifying as NCS Semifinalists (15%).

CCI NoVa Node also supported CyberSlam 2023, which brought together members of the Secret Service, Homeland Security, high school teachers, George Mason University faculty, and more than 400 hundred students from five counties and 22 high schools from the region to participate in a hands-on cybersecurity event. Additionally, CCI NoVa Node is sponsoring an experiential learning program for 18 high school students, focusing on cybersecurity and skills building, at University of Mary Washington, to be held in July 2023.

CCI NoVa Node is also represented on the commonwealth's Computer Science Education Advisory Board, helping with updated recommendations for Computer Science education standards for k-12, via program manager Jordan Mason.

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.

- **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.

3.2.3 SWVA Node

The SWVA Node funded 18 workforce programs:

- **Pathways for Cyberbiosecurity Workforce Preparation: Integrating Insights from Both Cybersecurity and Biosecurity**. Cyberbiosecurity is an emerging field at the interface of the life sciences and the digital world, and workforce development in cyberbiosecurity is a critical need in Southwest Virginia. Our specific aims for this project are: (1) crosswalk educational standards for biosecurity and cybersecurity into a comprehensive and integrative framework for cyberbiosecurity education, and (2) synthesize/analyze stakeholder perceptions that may guide curricular planning for cyberbiosecurity education, and (3) map potential on-ramps and off-ramps for cyberbiosecurity workforce preparation programs. The findings will provide information for future mapping of potential on-ramps and off-ramps for cyberbiosecurity workforce preparation programs and inform future innovations in post-secondary education, as higher education seeks to continually fill gaps in career preparedness in the most emergent and urgent fields.

- **Enhancing Cryptography Education using Collaborative Visual Programming**: Cryptography is the science of securing sensitive information and ensuring that only the intended recipients can access and process the encrypted data. It has become increasingly important to introduce the science of cryptography to future generations, at a younger age, in straightforward and more engaging ways. To achieve this goal, students need to acquire multidisciplinary skills in mathematics, information theory, and software programming. In addition, students must receive formal training in software testing and big data analysis. These requirements might create a barrier for non-computer science students and domain scientists to develop novel encryption algorithms or enhance existing ones. As a response, we have implemented a web-based programming learning tool called vizLab. The tool helps students bridge the gap between cryptography's mathematical foundations and computing by using a visual approach to programming. Students can learn to construct data encryption algorithms with minimal programming experience, using graphical icons representing the language's essential elements.

- **Secure mission-critical systems training: A SmartGrid Use Case**: The Secure Mission-Critical Systems Training: A SmartGrid Use Case project proposed a HS training program for cybersecurity. Our studies highlighted the inefficiency of relying solely on online materials for training in complex systems involving physical and digital resources. It emphasizes the need for a mix of factors like physical resource access, immersive training environments, mentorship, and interactive attack-defense scenarios to effectively raise cybersecurity awareness. During the senior mentors, such as graduate students, were assigned to undergraduate student groups at Virginia Military Institute (VMI), aiding their learning experience. The mentors also guided them in becoming future educators for younger H.S students. The project used cadets from VMI, undergraduate and graduate students from Virginia Tech (VT), who underwent intensive training to build a testbed for smartgrid facilities. The training covered software development, system design, hardware programming, VR implementation, cyber security investigations, vulnerability analysis, and creating attack-defense scenarios. Following the training, teams specializing in software, hardware, and XR technologies refined their designs and successfully built a functional testbed mimicking the smartgrid testbed with 2 houses and 3 power generation modules. The system was controlled using MQTT protocols, with web-based and XR-based frontends implementing the digital twin concept.

- **Global Center for Automotive Performance Simulation Internship Program**: This project supports 4 undergraduate interns to conduct a literature review on a cybersecurity topic. The 4 interns are divided into two groups. One group will research highway infrastructure cybersecurity concerns as it relates to automated driving systems (ADS). The second group will investigate cybersecurity topics centered on personally identifiable information (PII) within the context of healthcare. The outputs of

each effort may result in standalone, publishable works or be factored into future research proposals on these topics. In addition to the knowledge gained via the research effort, the intern participants will learn valuable skills for conducting academic research including technical writing, resource identification and citing, and experience common professional software suites.

- **Security Clearance Ready Certificate (SCRC) Program**: Security Clearance Ready Certificate (SCRC) is a program that informs undergraduate and graduate students about and prepares them for the security clearance process. The SCRC program is available to all students at CCI SWVA institutions. Students are required to attend four seminars during the academic year to earn the SCRC. There will be many opportunities to participate in seminars via virtual platforms (such as zoom) or in person. This program is designed to demystify the clearance process and streamline pathways between higher education programs and jobs requiring security clearance. Forty students participated and five certificates were issued.

- **Technology Enabled Engagements w/ Mentoring (TEEM) 2023**: Virginia's colleges and universities provide valuable knowledge to students. However, employer surveys routinely show that students from traditional programs are not workforce ready upon graduation. This is due to a lack of both critical thinking/soft skills and the inability to apply theoretical or abstract knowledge learned in the classroom. The goal of TEEM is to deliver structured and supported, technology-driven work/experiential learning opportunities that build students' technical and professional competencies via interactions with real-world professionals. TEEM will enhance students' high-quality traditional education with workforce-ready skills: critical thinking/soft skills and applied knowledge; by delivering an immersive industry work experience and mentoring relationships. To accomplish this, each week's student/mentor meeting features a different cybersecurity topic and the student 'owns their learning' which consists of working with the professional to establish a routine meeting time, studying weekly topic-related materials (written, video and interactive), and attending all mentor and program meetings1. To facilitate student success and maximize the mentor engagement, the student models professional behaviors via a provided set of detailed instructions and a highly structured agenda that they will follow for each week's meeting. Via the agenda the student will discuss the week's subject matter with the professional as well as ask related interview and feedback questions. All structured agendas, weekly topic information, and learning materials will be available within the online YourCareerCounselor platform. Answers/feedback from each weekly session, along with reporting on what went well and where the student can make improvements, will be recorded within the online platform by the student.

- **Broadening Participation in Security**: 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.

- **Women in Security**: The CCI Southwest node network has exceptional and diverse talent that could serve as role models, including leaders in several research areas. Moreover, it has existing collaboration with Virginia Tech's National Security Institute and a number of research centers which support diverse populations of students, scientists, and engineers. This program seeks to centralize that expertise in a mentoring network to provide encouragement for staying in the discipline. The purpose of Women in Security is to create a network of support and mentorship by successful women researchers.

- **Cybersecurity Competition Capacity Building: CTF Author Interns**: The Virginia Cyber Range organization hosts various collegiate and high school competitions in Virginia and elsewhere as outreach activities to help encourage students to explore cybersecurity topics, or simply as a competitive

venue for students already studying cybersecurity. Educators who use the Virginia Cyber Range platform can also host their own CTF competitions, and import challenges from a large library that we curate for their use. Since the same students will compete in different cyber range-hosted competitions year-after-year, we have to keep a steady supply of fresh challenges to maintain student interest. Furthermore, for competitive (prize awarding) events, we need new challenges to ensure that some teams don't have an unfair advantage for having seen a challenge in a previous event. This proposal is to sustain our capability to provide new and interesting CTF challenges by employing student interns that have CTF experience and requisite skills. We have had great success with students in this role and hope to continue this.

- **Virginia Cybersecurity Education Conference Teacher Sponsorship**: 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. High school cybersecurity educators sometimes do not have funds to attend these conferences. In an effort to defray costs for high school teachers whose schools are unable to pay for their conference attendance, we partnered with CCI to fund their participation. This project covers some of those travel costs. Conference registration includes Continuing Education Units (CEUs); many states, including Virginia, require teachers to earn professional development hours such as CEUs to ensure that teachers are up to date on current teaching practices and pedagogy. This investment in the future of K12 cybersecurity education in Virginia helps feed the pipeline of students into cybersecurity and STEM programs at CCI member institutions and other Virginia colleges and universities.

- **HBCU Quantum Partnership Workshop**: The 2023 workshop will build on successful funding proposals that were submitted as a result of the 2022 workshop. These proposals teamed Virginia Tech and Virginia State University (VSU) to establish a QISE experiential learning laboratory at VSU in 2023 and also ongoing funding proposals with both VSU and Prairie View A&M University (PVAMU) to 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. In fact, the 2022 and 2023 workshops will be a strong selling point for the ongoing funding proposals. Best practices for equitable HBCU partnering will result from the 2023 workshop since more careful input data from a larger group of HBCUs will be collected. Speakers from Virginia Tech, HBCUs, and other leading QISE research organizations will participate in the 2023 workshop.

- **Resilient and Secure BattleDrones: Drone Racing League for Southwestern Virginia**: The BattleDrones program aims to grow a statewide ecosystem of excellence in cyber-physical systems and serve as a catalyst for research, innovation, talent development, and commercialization of technologies at the intersection of security, autonomy, and data. The competition is designed to engage students from institutions across Virginia in autonomous systems and the data and algorithms that drives them. Competing institutions get the opportunity to provide students with training in Computer Vision, Artifice Intelligence, Machine Learning, and a platform to incorporate these algorithms into a single autonomous system. The objective of this program is to engage student in these advanced topics earlier in their educational program. The three focused objectives are on Recruitment, Cybersecurity Research, and Training. In the BattleDrones competition, teams will build and program a drone to fly autonomously through the designed obstacle course. Teams will be provided a drone kit which includes all a BOM and the core software to enable autonomous flight. From provided training videos, students should be able to assemble the drone and program it to successfully fly the course. The final competition will be in April 2023 when each competing team will race in the VT drone cage to see which team built the best system.

- **Undergraduate Research Experience**: This project allowed Radford University undergraduates to work on a CCI SWVA research projects at Virginia Tech. The students were integrated into the project. Team members researched, proposed, and refined research questions answerable using the

Open Source Intelligent (OSINT) collection engine. The students performed tasks and were part of the student team on the Cyber VIP: Use & Abuse of Personal Information project led by Dr. Alan Michaels.

- **Experiential Learning Mini-grants in cyberbiosecurity and data analytics in agricultural and food systems - Phase II**: Data analytics and security are essential topics for students in agriculture and the life sciences; these students must be prepared to analyze and protect life science data in associated industries. While a few undergraduate courses introduce related concepts, greater effort is needed to reach the broader agricultural and life science student population. This initiative provides mini-grants to support experiential learning for developing cyberbiosecurity and data analytics case studies, course modules, or experiential learning opportunities for agricultural and food systems-focused community college, undergraduate, and graduate courses. A request for proposals was distributed in Fall 2021 for experiential learning materials developed by graduate students with mentoring from VT Center for Advanced Innovation in Agriculture (CAIA) affiliate faculty and faculty at other CCI-affiliated institutions. Four proposals were received and three proposals were funded (two from CCI funding; one from CAIA funding). A second RFA was distributed in January 2022 for faculty to address course module development. Seven proposals were received and six proposals were funded. Three projects were directly funded through CCI Southwest and three were funded through CAIA resources. Projects ranged from data analytics for animal agriculture, soil chemistry, and food processing to cyberbiosecurity for agriculture and food science students. Projects involved faculty and students from Virginia Tech, Radford University, Lord Fairfax/Laurel Ridge and Virginia Western community colleges. Learning materials from each project were developed and shared through open educational resource options.

- **CCI SWVA/Industry Internships**: Internships were supported at 2 companies. ArchiveCore is a professional identity management platform that uses blockchain technology to simplify the professional credentialing process. The other company provides a comprehensive platform for network security, monitoring, and detection by deploying network and data traffic analysis. These internships funded 8 students from SWVA.

- **CCI SWVA interns**: During the 2023 fiscal year, the CCI Southwest Virginia office hired, onboarded, trained, and worked with two undergraduate student interns: a communications intern and a project management intern. The communications intern spent two semesters (Fall '22 and Spring '23) assisting with marketing and social media content for CCI projects, events, news, opportunities; assisting with story development to be published via VT news; assisting with event planning and special projects; and exploring cybersecurity communications as a career path. The project management intern spent Spring '23 learning about program management, project management, and research administration for a statewide initiative. Tasks included assisting with developing and implementing programs for the initiative such as workforce development programs, innovation programs and research programs for CCI SWVA; assisting with automation of CCI SWVA's reporting system; and assisting with event planning and special projects including: annual meeting, seminars, and student showcases.

- **CCI SWVA Outreach**: CCI SWVA supported many events to promote our three mission lines. We sponsored an event at the Roanoke-Blacksburg Technology Council to celebrate the 30-year anniversary of the Web. We gathered with technology companies and promoted our subsidized internships. We provided support for the CCI Integrated Seminar Series in the Fall, the ACTiV(T): Algebraic Coding Theory in Virginia (Tech), four sessions of the MAGMA for Coding and Cryptography Workshop, the Secure and Trustworthy Data and Technology Workshop and the CCI SWVA-PEC Workshop on the Cybersecurity of the Power Grid. These events help promote CCI SWVA, our research, workforce and innovation mission lines.

- **CodeVA Support**: The purpose of this program is aligned with the stated goals of Virginia state agencies, including Workforce, Commerce and Trade, Virginia Department of Education, SCHEV and others, to broaden and increase participation in Virginia's computer science/cybersecurity and adjacent technology workforce. Presently, Virginia faces a combined deficit of more than 100,000 workers to fill existing Virginia jobs in these fields. CodeVA is a state-funded program, designated through budget

legislation, to support the K-12 computer science and computational thinking Standards of Learning, which includes a specific K-8 strand and pathway courses focused on cybersecurity. CodeVA helps educate and prepare the pipeline to Virginia Universities by helping to prepare high school students. They are unique in that they serve all of Virginia high schools, and each Node of CCI sponsored this program in FY23.

3.2.4 Central Virginia Node

The Central Virginia Node (CVN) supported an Experiential Learning Call for Proposals and Internship programs at VCU and UVA and funded three projects at $50,000 each.

- **Secure Mobile (iOS) Programming through Experiential Learning**; Dr. Eyuphan Bulut, VCU; The proposed program aimed to train the students by teaching them not only the fundamentals of mobile iOS app programming but also the secure programming ways. Our target population was a cohort of students from both VCU and VUU. The program was open to students with all backgrounds with some prerequisites satisfied. Our goal was to expose the students who would normally not have much chance to take such a class but have abilities and skills. We met with students weekly over 10 weeks both in Fall 2022 and Spring 2023. There was a total of at least 20 contact hours which included hands-on in class exercises and assignments. The ultimate goal of the project was to increase the cybersecurity workforce in the mobile (iOS) app development industry by directing more students to this area. As a result of this project seven students earned certificates and the project has been funded for FY24 by the Hub.

- **Experiential Learning Through Exploring Deep Learning for Wireless Security**; Zhao, UVA; The objective of this project is to provide a great training and learning opportunity for both undergraduate and PhD students in exploring machine learning for wireless security. Two undergraduate students from VSU and two PhD students from VCU have participated in this project. Wireless signal quality plays a critical role in wireless security while wireless signal often deteriorated during the transmission by many factors. Therefore, a signal enhancement technique is desirable. In this study, we have trained students to formulate the wireless signal enhancement process as an adversarial learning problem and inspired them to develop a novel approach based on conditional Generative Adversarial Networks (cGAN). Unlike traditional signal denoising methods that estimate the noise or interference in the noisy signals, our proposed method estimates and learns the features of real noise-free signals, which is more adaptive to dynamic wireless communication environments. Students have conducted extensive simulations on noisy signals with four different modulations at different SNR levels. The results demonstrated that our proposed method was able to improve signal strength in a learning manner and achieved better performance compared with two traditional signal enhancement algorithms. Students have gained the skills how to apply machine learning to wireless security improvement.

- **Experiential Learning in the Development of Conformal 5G, 6G, and NextG Shielding Materials for Cyber-Physical Security Applications**; Dr. Ravi Hadimani, VCU; Two students from VSU, two students from VUU, and two students from VCU will be recruited as summer interns and trained in the development and characterization of the 5G/6G and NextG shielding materials at the Materials and Manufacturing Research Center of the Department of Mechanical and Nuclear Engineering and at the Department of Electrical and Computer Engineering. Students will also be offered an online course on electromagnetic shield technologies by Dr. Barua and Dr. Hadimani. Ultra-thin conformal coating materials for broadband electromagnetic wave (EMW) absorption are increasing day by day for military/defense and many potential applications to protect against electromagnetic threats. To address this need, 'summer internship experiential learning' in the development of novel, lightweight, economical 5G/6G and NextG shielding materials that conform to complex surfaces is proposed. In addition to receiving hands-on training on the synthesis and characterization of novel materials, the summer interns will also learn to use the tools available in the NextG Test bed of CCI at VCU. A visit to CCI's 5G/6G test bed located in Arlington, VA is also planned for the internship cohort. Finally, students will be given the opportunity to propose and work on a short project on their own at the end of their internship and to present the results from the project at the annual CCI

symposium. Student will also be encouraged to attend future CCI Cyber Camps. As a result of this project, two students have been recruited at both VCU and VSU.

Chapter 4

CCI Innovation

This chapter summarizes the main achievements in FY23 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 FY23 the CCI Hub began 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 the Northern Virginia, Central, and Southwest Virginia Nodes where six different Virginia-based venture capitalist companies were represented:

- Dreamit Ventures
- Data Tribe
- Blu Ventures
- Squadra
- Midland Capital
- Activation Capital

In FY24 meetups are scheduled at all four regional nodes.

4.1.2 Virginia Cybersecurity Challenge

At the 2023 Annual CCI Symposium, we announced the winning teams from the Virginia Cybersecurity Challenge. The winning teams, NetworkSense from VMI and Electrodefense from VCU began the final commercialization phase of the challenge. CCI partnered with US Ignite to launch a gated, four-phase innovation challenge in May 2021. The challenge began with six teams in 2021 with the ideation phase, moving through subsequent stages including prototyping, development and finally, commercialization.

Network Sense offers a web-based modeling and analytical environment for running network dynamics and predicting the spread of malicious behaviors and computer viruses on communication networks. Network Sense comes with a portal that hosts learning resources and educational materials. The company plans to offer packages with different combinations of their product's features to customers in 5G network security. The Market Research Future, a leading research firm, estimates that the global revenue of the 5G security

market will reach more than half a billion dollars by 2026. The company comprises an assistant professor at VMI, Dr. Sherif Abdelhamid, one recent graduate and one current undergraduate student.

Electrodefense created a multifunctional coating that can provide high-frequency electromagnetic radiation shielding and passive thermal management to prevent electromagnetic sabotage of wireless components. ElectroDefense plans to generate revenue by licensing the technology to companies in the IoT field. Over the long term, the solution can potentially have an impact on every network-connected device (IoT) — a market that Cisco estimates to be worth $14 trillion in 2022. The company comprises one assistant professor at VCU, Dr. Radhika Barua, and two undergraduate students.

The program was designed to guide researchers through the commercialization process and we are thrilled with the outcomes.

4.2 Node-led Programs

In addition to the CCI network-wide programs the Hub administered, the CCI Nodes also funded several innovation programs. Spending in FY23 across all nodes was $1,237,750.00 and is depicted in the chart below.

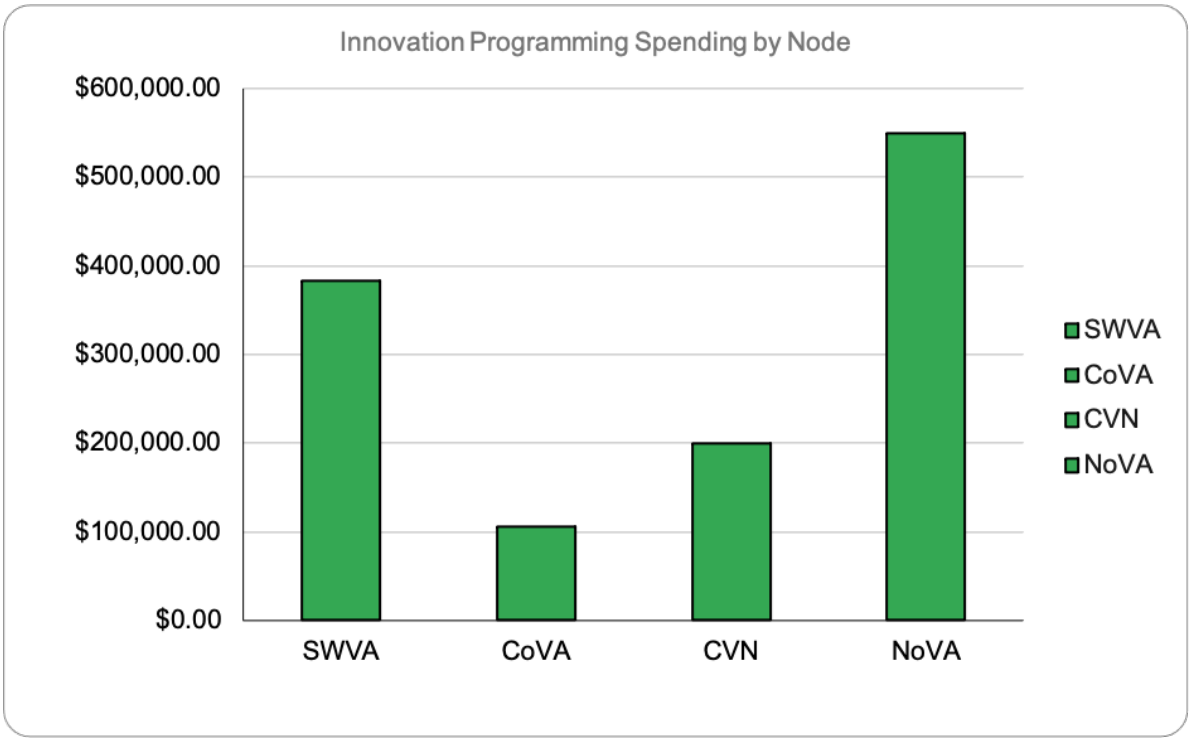


Figure 4.1: Innovation spending by node in FY23.

4.2.1 Northern Virginia Node

In FY23, 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 FY23, 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 compa-

nies 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 FY23, 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. Companies from previous cohorts have attracted over $1.2 million in new funding during FY23. In FY23, twenty-three cyber companies have engaged with ICAP.

- **Cyber Acceleration, Translation, and Advanced Prototyping for University-Linked Technology (CATAPULT)**. In 2023, 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 FY23 of $50,000 each. An investment of $250,000 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:

  - *Calibrating Trust in Human-Machine Interactions with Algorithmic Transparency;* George Mason University 12/1/22-12/31/23: AI systems have been increasingly used to facilitate human life, such as assisting people in complex daily tasks and boosting their productivity in the workplace. Most commonly-seen interactions between humans and machines are in one shot – humans send a task request and the machines complete the task by taking decisions and responding with the decision outputs. However, such one-shot task completion, coming with no follow-up human-machine interactions (e.g., humans validating the machine decisions), could expose humans to insecure situations, as even state-of-the-art AI systems could make mistakes in practice. This work is constructing a systematic framework for secure human-machine interactions. By focusing on "algorithm transparency", this work seeks to calibrate human trust with the reduced machine error rate and increased AI assurance and security resulting from this framework.
  - *Detecting Anomalous Virtual Reality Teleoperations via Artificial Intelligence;* George Mason University, Great Victory Legends, Inc. 5/12/23-5/31/24: With the rising popularity of virtual reality (VR) technologies, VR teleoperation of robotic systems has become increasingly popular in manufacturing, defense, healthcare, aerospace, logistics, etc. It is critical to enhance the cybersecurity of VR teleoperation systems to prevent hackers or other ill-intentioned users from maliciously controlling robots to cause damage on a remote site. This research works to devise AI to secure human-machine interactions, particularly in the context of VR teleoperation through the training of a deep reinforcement learning algorithm for detecting anomalous VR teleoperation. The algorithm forms the basis of an AI tool for monitoring and automatically detecting anomalous VR teleoperation patterns, whose occurrence would trigger a halt in the teleoperation, and inform cybersecurity operators to assume control – significantly enhancing the resilience, security, and reliability of different VR teleoperation systems.
  - *Development of Commercialization of Rapid Threat Assessment Tool for AI-enabled Systems;* George Mason University, Ampsight 5/12/23-5/31/24: The DoD, other government agencies and organizations in industries ranging from healthcare to financial services, and other critical infrastructure sectors must secure end-to-end machine learning (ML) systems against various new threats to achieve trusted AI. In the case of the DoD, the current Department of Defense (DoD)

Risk Management Framework (RMF) and accreditation process needs to be strengthened to assess an AI enabled system in a timely manner in order to grant Authority to Operate (ATO). The gap between AI/ML systems and the current security processes is a significant hurdle impacting mission. This project works to develop a minimum viable product prototype of a Rapid Threat Assessment Tool for AI-enabled systems.

- *Using Code-Glyph Mismatched Fonts to Protect Websites from Web Scraping;* George Mason University 5/12/23-5/31/24: Web scraping is a technology that uses automated crawlers to visit public webpages and extract text-based content data, and has wide-ranging financial implications. Studies show that e-commerce businesses lose 2% of online revenue due to web scraping, totaling over $100 billion in 2022. This research assumes a novel approach to combating web scraping by leveraging the mechanism of how characters are displayed in a web browser to ensure that humans can read appropriate context while a web crawler only obtains garbled text. Additionally, this approach prevents bots from extracting text by using optical content recognition techniques.
- *Next Generation Shielding Materials for Mitigating Intentional Electromagnetic Interference (IEMI) Cyber Threats;* Virginia Commonwealth University 5/12/23-5/31/24: As the paradigm of the Internet of Things (IoT) and Industrial Controls Systems (ICS) evolves into an essential component of modern life, securing its underlying cyber-physical systems (CPS) grows increasingly crucial. Nevertheless, Intentional Electromagnetic Interference (IEMI), one potential method for cyber attack trajectory, is often overlooked. IEMI has potential to damage critically important CPSes such as telecommunications, power networks, financial systems, medical devices, traffic control systems, manufacturing, mass transit, etc. Innovative electromagnetic shielding materials are poised to form the first line of defense to mitigate this threat, and are critical to the rollout of 5G technologies. This work aims to address the concerns of achieving broad bandwidth and confirming to logistical demands of 5G devices by developing a lightweight, conformal weather-resistant coating for broadband electromagnetic wave absorption in a target frequency range.
- *A Holistic Evaluation Framework for Multi-Modal AI Security and Trustworthiness on Federated IoE;* Old Dominion University 5/12/23-5/31/24: Emerging AI-enhanced Internet of Everything (AIoE) technologies have been incorporated into numbers CPSes to improve their operational efficiency and safety. While AIoE has achieved proven success, it requires vast amounts of training data for competitive performance. However, traditional centralized learning frameworks for AI raise privacy concerns due to the potential for sensitive information to be contained in the training data, making it an increasingly attractive target for cyber criminals. This research works to build a holistic evaluation framework for Multi-Modal AI Security and Trustworthiness on Federated AIoE.
- *Cybersecurity Awareness, Education, and Workplace Training Using Socially-enabled Intelligent Chatbots;* Virginia Military Institute, Virginia Tech, George Mason University 5/12/23-5/31/24: In the last decade, chatbot technology has emerged as a new area of AI, with use cases emerging across a spectrum of sectors. However, the application of intelligent agents in cybersecurity is still underrepresented. As cyber-attacks increase daily, very little work has focused on the prevention of human-induced attacks, whether unintentional or intentional. Traditionally, employers and organizations provide cyber awareness training to address the above issues. However, this is usually a one-time process, and does not provide necessary continuing support or education. This project focuses on how to secure such human-machine interactions through socially enabled intelligent chatbots, which will provide continuous support to users by providing immediate answers and guidance on how to navigate various threatening situations.
- *Generative Adversarial Network for Deep Learning-based Malware Detection Intellectual Property (IP) and Commercialization;* Christopher Newport University 5/12/23-5/31/24: The generative adversarial network (GAN) has been successfully applied in many domains in the past. GAN provides a new approach for solving computer vision, object detection, and classification problems by learning, mimicking, and generating any distribution of data. One of the difficulties in deep learning-based malware detection and classification tasks is lacking training malware samples. With insufficient training data, the classification performance of the deep model could be

significantly compromised. This research leverages GAN technologies to generate synthetic malware samples to increase training data and improve deep learning-based malware detection and classification.

  - *GoXG: A Novel Ultrafast GPU-based Scheduler Design for NextG Communication System;* Virginia Tech 5/12/23-5/31/24: The latest advancements in high-quality communication systems have resulted in the deployment of 5G networks, with next generation systems already being in design. Due to this dynamic network environment, coupled with diverse user needs, service providers must adapt their communication networks to ensure that end-users receive the best possible service. This requires a real-time to achieve (near-) optimal performance, in terms of high throughput, low latency, and low energy consumption, amongst others. However, meeting the requirements of real-time and (near-) optimal performance simultaneously is a significant challenge. This work assumes a novel approach to address this issue, resolving a number of the logistical challenges that hinder meeting these requirements.

- **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 2023, with proposals due March 1, 2023. Eight new companies and faculty partners were notified of their successful selection for CATAPULT funding in April 2023. In FY 23, one (1) new patent is pending as a result of CCI NoVa Node research endeavors: 1. Automatic Detection of Finger Photo Presentation Attacks, Emanuela Marasco (George Mason University), 2. Detecting Object not Visible in Color Images, Yongxin Wang and Duminda Wijesekera (George Mason University), 3. Countering Autonomous Vehicle Usage for Ramming Attacks, Duminda Wijesekera, Steve Kan, Zoran Duric, and Fernando Camille (George Mason University)

4.2.2 Coastal Virginia Node

- **INNOVATE Cyber**: CoVA CCI expanded the scope of the Innovate Cyber Challenge to include students from all state public 2- and 4-year institutions with the goal of selecting 50 students. This program groups students into teams and each team is assigned a cybersecurity problem/challenge. Over the course of 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 2023.

4.2.3 Southwest Virginia Node

The Southwest Virginia Node funded eight programs under the innovation and commercialization mission line.

- **Protecting Bystander Visual Data Privacy in Augmented Reality Systems**. In this project, we aim to design, develop, and prototype the first practical bystander privacy protection system that can effectively protect bystander visual (camera and depth) data privacy in real-time without negatively impacting user experience in Augmented Reality (AR) systems. The product will be a privacy-preserving API that sanitizes bystander information from sensor data streams before they are accessed

by third-party applications. At a high level, it modifies how third-party applications access raw visual data, identifies and obscures the bystander's faces, and passes on the obscured frames to the application.

- **Student Entrepreneurial Ideation Challenge SEIC 2023**: Incubators, accelerators, and entrepreneurial/small business development centers help budding entrepreneurs grow promising ideas from concepts into a business. These centers can be key to the entrepreneurial process but require innovative ideas for them to operate and achieve intended outcomes. While most entrepreneurial programs include 'ideation' as a critical first step in the process, it has not been robustly promoted or supported. As a result, an unintended barrier-to-entry can arise that may deter many students from pursuing Entrepreneurial careers. A core component of the entrepreneurial mindset is summarized with the statement, "People don't buy products. They buy solutions to problems." With this mindset, pursuing solutions requires first discovering the underlying problems that potential customers are experiencing. The Student Entrepreneurial Ideation Challenge asks student teams from higher education institutions to team up to respond to an industry challenge. The goal of the SEIC is to provide a robust, guided entrepreneurial ideation experience for students that will support the discovery of cybersecurity solutions/business ideas and promote an exciting and inclusive beginning for students' entrepreneurial journeys.

- **Power system reLiAnt Technology for Massive INterconnection of Integrated ReNEwables (PLATFORM-9)**: The transition to renewable energies is of course exciting, but it presents a humongous challenge for the power grid operations (utilities, independent system operators [ISO], and regulatory bodies). Before any new generation device (e.g., solar farm) is allowed to connect to the grid, its interactions with the grid under several scenarios must be thoroughly studied. These engineering studies are called "generation interconnection studies" (GIS) as defined by IEEE/ANSI standards and FERC/NERC (Federal Energy Regulatory Commission) regulations. The studies seem to be straightforward, but they are not. First, they are repetitive and time-consuming; some simulations take hours to complete and there are hundreds of such simulations, each varying one or two parameters, that are needed to complete the study. Second, data and system models are often not complete or are out of date, which leads to an inconsistent and incoherent representation of the system; finding these inconsistencies is difficult. Third, the US grid has system operators that are geographically dispersed; while they all operate under the FERC mandates, their operational practices sometimes differ significantly. Keeping track of such industry knowledge is a mobility constraint. Our goal is to create an automated system for (i) validating the consistency of the models and data, and (ii) performing the mandated studies (e.g., GIS) and additional advisory studies (e.g., cybersecurity studies). As of now, no company has a ready-to-use simulation platform and in-house expertise for all the electricity markets in the U.S. Similarly, no company exists that is specialized in running these studies and can provide a holistic and A-Z solution for all the electricity markets. At the same time, it is too early and risky for the big companies to fully engage in developing such a simulation platform.

- **Anti-Counterfeiting Authentication App Using Deep-Learning-Based Physically Unclonable Functions**: Counterfeiting is an increasingly prevalent global issue, threatening the health and safety of individuals, corporations, and nations. Several legal measures have been implemented to secure product legitimacy but fall short of offering a user-end safeguarding mechanism. This project proposes a mobile application to authenticate products using previously researched security labels. These labels utilize an innately random property of silk proteins to create a unique identifier called a physically unclonable function (PUF). A machine-learning-based key generation algorithm, involving some image pre-processing steps, deep-learning prediction, and randomness extraction techniques, is then used to generate a key of 0s and 1s. This binary key is suitable for cryptographic applications. The objectives of this project are to determine a sufficiently secure, suitable authentication protocol for validating generated keys and build a reliable, resilient user-end mobile application prototype for validating PUF label authenticity. In the previous phase of this project, the cryptographic keys generated from the unique PUFs were sufficiently random and thus cryptographically secure, evaluated using the NIST SP 800-22 Statistical Test Suite. The impact of the proposed project is driven by human factors and global security, aiming to safeguard industries and consumers from counterfeiting

threats. The expected outcomes from this work are to survey bio-PUF authentication protocols and to prototype a mobile authentication app using both uploaded and phone-camera-captured PUF label images.

- **Cyber RADaR (Cybersecurity Rapid Asymmetric Discovery and Reporting) Phase Two: Commercially Deployed Beta Product**: Most cyberattacks are inherently asymmetric, targeting security vulnerabilities that "inflict a proportionally large amount of damage compared to the resources needed" to commit the attack. Until a patch is available, interim remediation to combat asymmetric cyber threats can be particularly complex for professionals, especially in small and medium sized organizations. Technology and cybersecurity professionals have increasingly turned to online social media to share and consume the latest threat information with a particular focus on understanding and remediating zero-day threats. Using online social networks is not new. In fact, social networks are becoming the primary source for threat remediation support. To better understand and address the need to use social network data for cyberthreat identification and remediation, our project team completed an initial project sponsored by SW CCI: Cyber RADaR: Cybersecurity Rapid Asymmetric Discovery and Reporting via AI-driven Social Media Crowdsourcing. During the phase one project, the team developed and validated a Cyber RADaR proof-of-concept (PoC) using advanced data processing techniques, including machine learning (ML) and natural language processing (NLP), to demonstrate the capability to automate the discovery, collection, transformation, analysis, and presentation of online social network (twitter and Reddit) sourced asymmetric threat data. The Cyber RADaR Phase 2 project seeks to enhance and expand phase one capabilities. Efforts to accomplish this will include: 1) additional development of new and existing algorithms; 2) functional and user experience (UX/UI) dashboard enhancements; and 3) the establishment of a customer feedback group to iteratively test and recommend product modifications.

- **Cyber RADaR (Cybersecurity Rapid Asymmetric Discovery and Reporting): Intellectual Property (IP) Registration**: The first phase of the Cyber RADaR project produced a proof of concept and the second phase will develop a prototype with input and guidance from industry partners. The Cyber RADaR: IP Registration project will provide initial protection for the intellectual property (IP) used by the CyberRADaR projects. As the project team begins to consult with external partners and begin product development, intellectual property must be protected. The project will protect IP by preparing and submitting trademark and provisional patent applications with the United States Patent and Trademark Office (USPTO). Trademarks and patents will be filed by CivilianCyber, which will offer IP protection for two brands: (1) CyberRADaR, and (2) the underlying WIaaS technology. CivilianCyber will work with Radford University to resolve any IP concerns. The project team has IP registration capabilities on staff and has added an IP registration expert consultant (Michael Miller) for further support. Each step, for both trademarks and patents, requires USPTO approval to continue the process and the process will end either when USPTO fully approves or denies the request. The primary performer of each step is listed after the step name but note that the project team will be in constant communication with the USPTO throughout the process to provide any feedback/clarifications.

- **Scalable Continuous Monitoring Solutions for Enterprise Security**: This commercialization effort aims to develop deployable continuous monitoring solutions for managing enterprise security against stealthy external and internal threats. The specific product that we envision is a piece of stand-alone monitoring software, tentatively named SoftAuditor. SoftAuditor aims to detect stealthy attacks and anomalies in an organization, e.g., due to advanced persistent threats (APT) such as SolarWinds APT, as well as malicious insiders that may cause data leak. SoftAuditor can be deployed on endpoints or in the cloud, making intelligent security decisions based on observed employee and system data. Our ongoing efforts are focused on developing solutions to support better forensic capabilities that are urgently needed for cybersecurity investigation by security analysts. Our work leverages our existing malware detection expertise, as well as findings from our prior market research. Regarding potential clients and possible distribution mechanism, one direction is to explore the possibility of integrating our solutions to existing IT security frameworks and products as an add-on cybersecurity extension.

- **Cyber Innovation Scholars**: A group of 24 doctoral candidates, master's students, and postdoctoral researchers attended the first ever Cyber Startup Lab where they were introduced to processes

involved in commercializing cyber technology. The 2023 Cyber Innovation Scholars hail from departments across Virginia Tech, including agricultural, leadership, and community education; computer science; electrical and computer engineering; food science and technology; 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 three calls for proposals to support Innovation and Commercialization: a node-wide call, an internal UVA call*, and a Dreams to Reality Incubator call (limited to VCU PIs)**. Overall, eight projects were supported totaling $200,000.

- **Vision-based Passive Micro-movement Sensing System for Telehealth**; Dr. Seongkook Heo, UVA; While online meeting systems have been heavily adopted in our lives, virtual doctor visits are not always effective, due to the difficulty of making physical examinations and the lack of sensing equipment on the patient's environment. This project develops a new and affordable sensing method that can measure forces and micromovements using a passive device and a webcam of a laptop or a mobile device, so that virtual doctor visits can be more effective. We created MoireTag, a device that contains a small structure frame with stripe-pattern slits, a sliding paper with stripes pattern printed on it, and an elastic rubber module that creates a compliant movement. We developed a computer vision algorithm that detects the MoireTag in a video feed, crops the window region, and extracts the Moire Fringe movement. Our validation showed that MoireTag could reliably detect sub-mm movement in real time (mean detection error = 0.04 mm) when used with a consumer web camera. We also show that MoireTag connected to a strap worn on a user's chest can detect breathing of the user at an average of 99% of accuracy in real time.To demonstrate the potential use of method, we developed custom remote meeting systems that can allow users to bring physical objects into online discussions and also automatically create visual overlays for MoireTag measurements of physiological signals. This team has collaborated with a researcher at Google, Dr. Ruofei Du, to develop a remote meeting system that can incorporate physical objects and measures.

- **Wireless Smart Home Intrusion Detector**; Dr. Eyuphan Bulut, VCU; In this project and commercialization effort, our goal is to leverage the WiFi networks and systems available in most houses for building a home security or intrusion detection system with the necessary functionality. This will reduce the hardware cost and minimize deployment efforts. Building on our various WiFi sensing based studies and utilizing our novel and standalone CSI collection tool that can run machine learning model inference onboard in real time using the collected CSI value, we aim to develop a standalone product and prototype. This can potentially supply the demand in the market for a low-cost home security system and increase the adoption of security systems at homes. Through collaboration with several VCU Computer Science Department Industrial Advisory Board members, we will proceed with steps towards comprehensive evaluation of the proposed product in various home environments and making it ready for commercialization.

- **Towards Real-Time Federated Learning over Wireless Communications**; Dr. Cong Shen, UVA; We start building a real-time federated learning (FL) prototype system over a real-time wireless communication system. Such prototype represents a first step towards building an intelligent Internet of Things (IoT) system that can enable machine learning (ML) technologies at the end IoT device through commercial wireless communication systems (such as 5G). We studied a new problem in federated multi-task learning (FMTL) where each task may be performed at multiple clients and each client may perform multiple tasks. The novel insight is that the distribution of features may vary across different tasks at different clients. Such feature heterogeneity offers a new opportunity to improve the generalization capability of FL. We analyzed the ML model convergence of a new hybrid learning architecture, which leverages the server dataset and its computation power for collaborative model

training with clients. Different from FL where stochastic gradient descent (SGD) is always computed in parallel across clients, the new architecture has both parallel SGD at clients and sequential SGD at PS. We analyze the convergence rate upper bounds of this aggregate-then-advance design for both strongly convex and non-convex loss functions.

- **Prototyping Data-driven Cyber-Attack Detection Techniques in Autonomous Vehicle Cyber Physical Systems**; Dr. Haiying Shen, UVA; As autonomous vehicles become a part of the landscape of Transportation Cyber-Physical Systems (TCPS), there are more questions than ever about their safety. Because of CAVs' interface with the outside-vehicle environment, the vehicle systems are much more open to the outside-vehicle environment, which increases their risks of being attacked. False information insertion is one type of attacks that may cause threat to driving safety and human life. For example, a compromised vehicle can also send a false emergency brake light alert to its follower vehicle, which may stop suddenly and leads to catastrophic rear-end collisions. The PI proposed a real-time false information detection system in V2V communication in her prior work. It checks the consistency between the estimated and actual reported driving states of an alerting vehicle and its nearby CAVs, and uses a machine learning (ML) method and enhances a traffic flow model for the estimation. To transition this research work to practice, the PI proposes this project to prototype the false information detection system. The prototype will be tested in the lab as well as in the controlled real-world environment. To measure the project success, we will use metrics including (1) the prototype's quantifiable effectiveness in detecting false information in V2V communication, (2) the additional overhead of the prototype, (3) whether the prototype is easy to be integrated to CAV, (4) whether the prototype is easy to use, and (5) the number of potential customers who will use the prototype. The team has created collaborative partnerships with Perrone Robotics, Inc. and have discussed with them about the possible adoption of the developed techniques after the techniques are fully developed and tested.

  UVA-funded projects were funded to toward proposals to federal innovation/commercialization funding sources, such as NSF I-Corps, NSF Partnerships for Innovation.

- **Connected Vehicle Identification System and Cybersecurity Assessment Testbed**; Dr. Brian Park, UVA; The main purpose of this project is to design, develop, and evaluate a prototype connected vehicle identification system. A previously developed and successfully tested algorithm using real-world vehicle trajectory data will be modified to work with the proposed prototype system. It is noted that the prototype developed in this project could serve as a cybersecurity testbed for future research. The proposed prototype will be based on off-the-shelf components, including the Jetson Nano board, GPS unit, Wi-Fi dongle, time of flight sensor, and lidar sensor. Each connected vehicle will be equipped with this prototype, except for an ego vehicle with a lidar sensor to measure the distance to the preceding vehicles and their speeds. We have successfully assembled the Jetson board, GPS unit, and Wi-Fi dongle and tested the communications between the Jetson boards. We are in the process of integrating a liar sensor to detect the preceding vehicles. The field evaluation will use real vehicles equipped with the prototype system and a lidar sensor at the ego vehicle. Tasks already completed include (i) setting up a vehicle ad-hoc network for vehicle-to-vehicle communications and (ii) parsing GPS measurements and adding them to the payload. The remaining tasks include (i) processing lidar sensor raw data to generate point cloud data for vehicle tracking and (ii) implementing the connected vehicle identification system.

- **Physics-Inspired Compute Engines for Accelerating Combinatorial Optimization**; Dr. Nikhil Shukla UVA; The investigator's team has recently developed a new class of physics-based solvers to solve hard computational problems in combinatorial optimization that are still considered intractable to solve using conventional digital platforms. Combinatorial optimization is a core computational primitive that is frequently needed in the computational backend of a wide range of applications spanning from resource allocation, autonomous vehicles, training of artificial intelligence systems to applications in finance such as portfolio optimization and arbitrage trading. Despite their extensive applications, developing efficient accelerators for solving such problems continues to be a significant challenge and constitute a major performance bottleneck for such applications. In fact, the relevance of solving such problems efficiently has spurred active interest and investment in new fields such as quantum computing, both from the government and industry. However, considering the special needs of this

technology such as cryogenic cooling, quantum computing, even if successful, will only be able to serve server class applications, and not applications at the edge that operate under energy constrained environments, possibly without cloud connectivity. In contrast, our proposed solution would provide a room-temperature technology with energy needs that are orders of magnitude lower than the large cloud-based solutions. Inspired by the team's new research results, the goal of this project is to advance the commercial potential of this technology by: (i) performing algorithmic adjustments to meet commercial applications. (ii) further optimize performance through hardware-algorithm co-design. (iii) Become competitive for larger commercialization grants.

*** VCU-funded projects were so PIs/co-PIs could pursue commercialization. This has resulted in the formation of two new spin-outs in CVN.*

- **RAM Phantom, LLC (https://www.ramphantoms.com/) Founder Ravi Hadimani**; Anatomically realist brain phantoms that mimic brain structure, electrical, magnetic, and mechanical properties are designed, fabricated, partially tested, and patented using CCI project funds. These phantoms, also known as Realistic Anatomical Model (RAM) phantoms, are fabricated using MRI images, novel polymer nanocomposites, and 3D printing for neuromodulation security and safety research and training. These phantoms are used in research to test intentional electromagnetic interference, unsafe induced voltages inside the brain, and new brain stimulation procedures. These phantoms can also be used in education for training brain stimulation clinicians, medical device security experts, and neurosurgeons. The PI, Hadimani, and his graduate student Wesly Lohr will standardize and simplify the fabrication of RAM phantoms and validate their safety and security on other neuromodulation procedures such as DBS and simultaneous TMS-DBS. We will then launch a company, RAM Phantoms LLC., to commercialize these brain phantoms. RAM Phantom, LLC has established a collaboration with an Assistant Professor at Harvard University to measure the effect of magnetic stimulation on a rat brain phantom and filed two new invention disclosures.

- **AIOTI, Inc. Founders Sherif Abdelwahed, Nathan Puryear, Ashraf Tantawy, and Stefano Iannucci**; In this project we working to develop a porotype of an extendable model-base home automation system and verify its functionalities and prove its effectiveness in the context of a real home operation environment. The proposed home automation system offers a complete solution for smart home management through its innovative, affordable and easy to use interface. In addition, it is expected to work with the with existing heating and cooling systems as well as various home appliances. The prototype will include the software system and a set of integrated IoT devices that optimize house performance with respect to various criteria related to comfort, cost-effectiveness, reliability/safety, and security. AIOTI, Inc. is working on a collaborative partnership with M.C. Dean, Inc.

Chapter 5

Collaborative Partnerships and Projects

5.1 Partnerships

5.1.1 Arlington County Smart Community Pilot

For nearly two years, Dr. Menon from Mason and who is sponsored by CCI, has been a partner in the pilot Safety and Innovation Zone (SIZ) project, along with Arlington County, non-profit US Ignite, and commercial service providers Comcast and Juganu and VT in year one. While the initial scope of work for the Mason team was directed to the SIZ privacy practices, the team was later requested to focus their attention on the project's data – to perform data privacy review, data evaluation and data analysis. In part, this adjustment was in response to input from community members with questions and concerns about the privacy and security protections around the new collection of sensor data. Key takeaways from this project include:

- Data privacy risk was successfully identified, assessed and mitigated for the project. A privacy-first approach can produce interesting data while still respecting privacy.
- Implementation of robust data privacy and security protections also introduced constraints around data management generally and perhaps avoidable data quality challenges.
- Assuming the County will continue to pursue privacy-impacting activities in the future, data quality and data privacy risk management should be considered at both the project and organizational level.
- Data analysis was constrained by sensor outages and data quality issues. Consequently, a determination has not yet been made as to how sensor data could enhance public safety incident response.
- GMU's scope of work evolution demonstrates the flexibility required when piloting new data-rich technology and also the County skills and/or capacity gaps to support this type of work operationally.
- The trust building activities among partners conducted throughout the project provided were critical to leveraging all the partners' skills and establishing the underpinnings for success with future initiatives.

The GMU team completed an initial body of work around data privacy practices employed throughout the planning and implementation phases of the SIZ project before shifting focus to data analysis the County considered critical to address the core question of the pilot project – can the sensor technology reliably provide enhanced insight into public safety events while protecting individual privacy? The contributions of the GMU team to identify data quality issues speak particularly to the "reliably" portion of the core question.

5.1.2 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.

5.1.3 VASEM Summit 2022

The Virginia Academy of Science, Engineering, and Medicine provides independent forums to exchange new ideas in science, technology, and medicine. One of these activities is its Annual Summit. The Virginia Academy invites researchers and innovators in Virginia to organize a Summit on topics that highlight emerging areas of importance for the Commonwealth. With the support and experience of Virginia Academy staff, the Summit provides a unique opportunity to bring visibility to current and emerging Virginia leaders in forefront areas that are vital to the Commonwealth.

In 2021, CCI was selected by the VASEM Board to host the 2022 annual summit. The Summit was held on October 25, 2022 at the National Academy of Sciences building in Washington DC. The summit topic was Securing the Future of Cyberspace. The topic was both timely and relevant because cybersecurity is critical and impactful to both the private and public sectors within the Commonwealth and beyond. The Summit agenda was a mix of eminent leaders and leading innovators as speakers and panel members, cybersecurity technology research poster presentations by CCI students, and opportunities for networking and socializing.

VASEM Summit Speakers

- Keynote: Dr. Robert Kahn
- Industry Spotlight: Mr. Dan Bono, Vice President Cyber Mission Operations CACI
- Fireside Chat: Ms. Kiersten Todt, Chief of Staff, CISA and Dr. Tom Dingus, Virginia Tech
- Panel: Securing the Next Generation of Networks, Ms. Debra Jordan, Dr. Charles Clancy, Dr. Sennur Ulukus

5.1.4 Industry-led Consortia

O-RAN Alliance

In 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

In FY23, CCI commissioned RTI International to conduct a second economic impact study for fiscal years 2022 and 2023. In FY21, RTI conducted CCI's first economic impact study for fiscal years 2020 and 2021. In FY 2022 and 2023, CCI continued its activities in research, workforce, and commercialization and, as seen in Table 16 below, showed significant growth from the prior years in areas of workforce and commercialization with more students served and more engagement with the startup ecosystem. CCI's research activities remained strong, continuing to support publications and engagement of new PIs and collaborators, and growing levels of leveraged external research funding. Below are some of the impact study highlights:

- In FY 2023, CCI researchers reported over $75 million in leveraged research funding, nearly double the annual total in prior years.
- In FY 2023, CCI supported a record 330 interns, the highest number since the start of the initiative.
- In FY 2022 and FY 2023, CCI reported continued growth of startup and patenting activities, directly supporting a total of 21 startups and 20 patent filings.
- Since 2020, CCI – supported startups reported a total of $3.8 million in venture capital raised and 13 jobs created.
- CCI workforce programs reported 45 direct full-time job placements.
- Since its inception, CCI has formed 652 external partnerships.

5.2.1 Economic Impacts of CCI Activities

CCI's activities in research, workforce, and commercialization support jobs, labor income, and economic activity across Virginia. To calculate their impact, RTI conducted analysis with an input-output model using IMPLAN to understand the contributions of CCI activities across the commonwealth and in the four regional nodes. The model includes the following measures:

- Jobs consist of all full-time, part-time, and temporary positions. Jobs are reported as an annual average. Direct jobs are those created with CCI funding such as program administrators, faculty, and program researchers. Indirect jobs are those supported by CCI program spending among local businesses. Induced jobs are supported by CCI employees and employees at businesses with CCI contracts spending their wages in the local economy.
- Labor income is a component of value added and represents multiple forms of employee compensation, including wages and benefits and proprietor income, which consists of income from self-employed individuals and independent business owners. Labor income indicates how much additional personal income is created by CCI activities.

Table 16. CCI Node Performance Metrics: FY 2020-FY 2023 Reported

METRICS REPORTED	FY 2020 REPORTED	FY 2021 REPORTED	FY 2022 REPORTED	FY 2023 REPORTED
Research				
Number of CCI-funded projects	36	88	46	101
Externally funded projects reported	172	112	87	116
Value of externally funded projects	$40 M**	$37 M*	$39.8 M	$75.1 M
Number of publications	58	111	119	168
Number of PIs and collaborators	236	321	103	99
Workforce and Experiential Learning				
Number of research scientists and graduate assistants	32	83	110	125
Number of interns and participants in experiential learning programs	-	92	151	330
Number of full-time job placements	-	-	45	-
Number of undergraduate students supported	-	235	243	323
Commercialization				
New startups directly supported	3	1	9	8
Number of participants in startup programming	-	33	137	23
New jobs created by startups	-	-	13	-
External funding raised for innovation/entrepreneurship programming	-	-	$2.4 M	$1.4 M
Number of filings for IP	2	5	7	6
Number of external partnerships	128	219	146	159
External venture capital raised by startups	-	-	$240,000	-

Source: CCI Annual Report FY 2020, FY 2021, FY 2022, Node Reports 2022, Node Reports 2023, Interviews with Node Program Managers and Staff

- Value added provides an indicator of the labor, capital, and tax income generated from production activities. It consists of a combination of labor income, proprietor income, and profits.
- State and local tax revenue is the sum of tax revenue that will be generated at the subcounty, county, and state levels. These taxes include items such as state income taxes, corporate business taxes, sales taxes, and special district fees.

CCI activities supported 619 jobs in FY 2022 and 889 jobs in FY 2023 through its activities and impacts to research, commercialization, and workforce development programming. By FY 2023, CCI's contribution to Virginia's GDP surpassed $100 million in value added and it had effects across the four regional nodes.

5.2.2 FY 2022 Activities

In FY 2022, CCI's activities supported a total of 619 jobs, earning an estimated $46 million in labor income and $62 million in Virginia economic activity, as seen in Table 21. These activities generated an

estimated $3.9 million in combined state and local government revenues, including an estimated $2.3 million in Commonwealth of Virginia revenues.

Table 21. Economic Activity Supported by CCI in Virginia in FY 2022

	Jobs	Labor Income	Value Add	Output	State and Local Government Tax Revenues
Direct	318	$27.4 M	$30.7 M	$58.1 M	$0.9 M
Indirect	155	$10.5 M	$16.2 M	$30.1 M	$1.1 M
Induced	146	$7.9 M	$15.2 M	$25.6 M	$1.9 M
Total	**619**	**$45.8 M**	**$62.1 M**	**$113.8 M**	**$3.9 M**

Source: IMPLAN, RTI analysis of FY 2022 CCI spending data.
Note: Columns may not sum due to rounding.

Jobs

In FY 2022, Virginia CCI spending directly created 318 jobs. Direct job creation was concentrated in scientific R&D services, at institutions of higher education, and in the computer system design support industry. For every direct job created by CCI, another position is supported in the wider economy through indirect and induced employment. The 155 indirect jobs are concentrated in industries such as real estate services, scientific R&D services, employment services, and management services. Induced jobs, which consist of 146 positions, were supported in the restaurant, retail, and health service industries. Altogether, approximately 619 jobs were supported by CCI activities.

Labor Income

In 2022, CCI activities supported $45 million in labor income and were the largest components of value added.

Value Added and Output

Value added and output are both ways to measure the size of specific industries and the economy. Value added provides an indicator of the labor, capital, and tax income generated from production activities. It consists of

- labor income (employee income + proprietor income)
- taxes on production and imports (taxes to operate a business and imports)
- other property income (dividends, corporate profits, interest earned on bank deposits, and reduction in value of fixed assets.

Value added is also referred to as contribution to gross domestic product (GDP).

Output is equal to value-added plus the value of intermediate goods and services. In IMPLAN, output is presented as annual production estimates for the data year. For service sectors, output equals sales. CCI activities created $114 million in output in 2022.

State and Local Tax Revenue

More than half of taxes are those collected at the state level, including personal income tax ($1.1 million) and sales tax ($0.9 million). At the county level, tax revenue is derived from property tax ($0.8 million) and local sales tax ($0.1 million). Finally, a small amount of tax revenue is raised by sub-county assessments including property tax ($0.4 million) and sales tax ($0.1 million).

Region-by-Region Breakdown - 2022

In each of the four regions served by the CCI nodes and hub, CCI activities contributed to jobs, labor income, output, and state and local government revenues. The 619 jobs supported by CCI are broken out in the following section, with the four nodes' contributions to their regions. Regional activities funded by the hub are allocated to the region where they took place, and direct hub activities in Northern Virginia are allocated to Northern Virginia. Regional economic impacts are found in Tables 22-25.

Coastal Region

Table 22. Economic Activity Supported by CCI Coastal in Coastal Virginia in FY 2022

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	45	$4.2 M	$4.9 M	$9.2 M	$0.2 M
Indirect	23	$1.4 M	$2.3 M	$4.3 M	$0.2 M
Induced	24	$1.2 M	$2.3 M	$4.0 M	$0.3 M
Total	**92**	**$ 6.8 M**	**$9.4 M**	**$17.5 M**	**$0.7 M**

Source: IMPLAN, RTI analysis of FY 2022 CCI spending data.
Note: Columns may not sum due to rounding.

Central Region

Table 23. Economic Activity Supported by CCI in Central Virginia in FY 2022

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	65	$6.3 M	$7.1 M	$13.7 M	$0.2 M
Indirect	37	$3.0 M	$4.5 M	$7.8 M	$0.3 M
Induced	41	$ 2.3 M	$4.5 M	$7.4 M	$0.5 M
Total	**143**	**$ 11.6 M**	**$16.1 M**	**$28.9 M**	**$1.0 M**

Source: IMPLAN, RTI analysis of FY 2022 CCI spending data.
Note: Columns may not sum due to rounding.

5.2.3 FY 2023 Activities

In FY 2023, CCI's activities supported a total of 863 jobs, earning an estimated $71 million in labor income and $97 million in Virginia economic activity, as seen in Table 26. These activities generated an estimated $6 million in combined state and local government revenues, including an estimated $2.7 million in Commonwealth of Virginia revenues.

Jobs

In FY 2023, Virginia CCI spending directly created 428 jobs. Direct job creation was concentrated in scientific R&D services, at institutions of higher education, and in the computer system design support industry. For every direct job created by CCI, another position is supported in the wider economy through indirect and

Northern Region

Table 24. Economic Activity Supported by CCI in Northern Virginia in FY 2022

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	114	$11.0 M	$11.8 M	$18.8 M	$0.3 M
Indirect	33	$2.7 M	$4.4 M	$7.5 M	$0.3 M
Induced	41	$2.5 M	$4.8 M	$7.8 M	$0.6 M
Total	**188**	**$16.2 M**	**$21.0 M**	**$34.1 M**	**$1.1 M**

Source: IMPLAN, RTI analysis of FY 2022 CCI spending data. Includes hub activities that take place in the Northern Virginia region.
Note: Columns may not sum due to rounding.

Southwest Region

Table 25. Economic Activity Supported by CCI in Southwest Virginia in FY 2022

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	94	$5.9 M	$6.8 M	$16.5 M	$0.2 M
Indirect	63	$3.4 M	$5.0 M	$10.6 M	$0.4 M
Induced	40	$1.8 M	$3.6 M	$6.4 M	$0.5 M
Total	**197**	**$11.2 M**	**$15.5 M**	**$33.5 M**	**$1.1 M**

Source: IMPLAN, RTI analysis of FY 2022 CCI spending data.
Note: Columns may not sum due to rounding.

Table 26. Economic Activity Supported by CCI in Virginia in FY 2023

	Jobs	Labor Income	Value Add	Output	State and Local Government Tax Revenues
Direct	428	$42.6 M	$48.6 M	$90.7 M	$1.4 M
Indirect	226	$16.9 M	$25.6 M	$45.9 M	$1.6 M
Induced	209	$11.7 M	$22.7 M	$37.6 M	$2.7 M
Total	**863**	**$71.2 M**	**$96.9 M**	**$174.2 M**	**$5.8 M**

Source: IMPLAN, RTI analysis of FY 2023 CCI spending data.

Note: Columns may not sum due to rounding.

induced employment. The 226 indirect jobs are concentrated in industries such as real estate services, scientific R&D services, employment services, and management services. Induced jobs, which consist of 209 positions, were supported in the restaurant, retail, and health service industries. Altogether, approximately 863 jobs were supported by CCI activities.

Labor Income

In 2023, CCI activities supported $71 million in labor income and were the largest components of value added.

Value Added and Output

Value added and output are both ways to measure the size of specific industries and the economy. Value added provides an indicator of the labor, capital, and tax income generated from production activities. It consists of

- labor income (employee income + proprietor income)
- taxes on production and imports (taxes to operate a business and imports)
- other property income (dividends, corporate profits, interest earned on bank deposits, and reduction in value of fixed assets.

Value added is also referred to as contribution to GDP. Output is equal to value-added plus the value of intermediate goods and services. In IMPLAN, output is presented as annual production estimates for the data year. For service sectors, output equals sales. CCI activities created $180 million in output in 2023.

State and Local Tax Revenue

More than half of taxes are those collected at the state level including personal income tax ($1.8 million) and sales tax ($1.3 million). At the county level, tax revenue is derived from property tax ($1.4 million) and local sales tax ($0.2 million) Finally, a small amount of tax revenue is raised by sub-county assessments including property tax ($0.4 million) and sales tax ($0.2 million).

Region-by-Region Breakdown - 2023

In each of the four regions served by the CCI nodes and hub, CCI activities contributed to jobs, labor income, output, and state and local government revenues. The 889 jobs supported by CCI are broken out in the following section, with the four nodes' contributions to their regions. Regional activities funded by the hub are allocated to the region where they took place, and direct hub activities in Northern Virginia are allocated to Northern Virginia. Regional economic impacts are found in Tables 27-30. The counties that make up the regions are detailed in Appendix B.

Coastal Region

Table 27. Economic Activity Supported by CCI Coastal in Coastal Virginia in FY 2023

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	44	$4.1 M	$4.7 M	$9.0 M	$0.2 M
Indirect	23	$1.4 M	$2.3 M	$4.3 M	$0.2 M
Induced	24	$1.1 M	$2.3 M	$3.9 M	$0.3 M
Total	**90**	**$6.7 M**	**$9.3 M**	**$17.2 M**	**$0.6 M**

Source: IMPLAN, RTI analysis of FY 2023 CCI spending data.
Note: Columns may not sum due to rounding.

Central Region

Table 28. Economic Activity Supported by CCI in Central Virginia in FY 2023

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	52	$5.1 M	$5.8 M	$11.0 M	$0.2 M
Indirect	30	$2.4 M	$3.6 M	$6.3 M	$0.2 M
Induced	33	$1.9 M	$3.6 M	$6.0 M	$0.4 M
Total	**115**	**$9.4 M**	**$13.0 M**	**$23.3 M**	**$0.8 M**

Source: IMPLAN, RTI analysis of FY 2023 CCI spending data.
Note: Columns may not sum due to rounding.

Northern Region

Table 29. Economic Activity Supported by CCI in Northern Virginia in FY 2023

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	228	$26.7 M	$30.3 M	$51.8 M	$0.8 M
Indirect	101	$9.2 M	$14.0 M	$23.2 M	$0.8 M
Induced	107	$6.6 M	$12.7 M	$20.4 M	$1.5 M
Total	**436**	**$42.5 M**	**$57.0 M**	**$95.5 M**	**$3.1 M**

Source: IMPLAN, RTI analysis of FY 2023 CCI spending data. Includes hub activities that take place in the Northern Virginia region.
Note: Columns may not sum due to rounding.

Southwest Region

Table 30. Economic Activity Supported by CCI in Southwest Virginia in FY 2023

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	104	$6.7 M	$7.7 M	$18.8 M	$0.3 M
Indirect	72	$3.9 M	$5.8 M	$12.1 M	$0.4 M
Induced	46	$2.1 M	$4.1 M	$7.3 M	$0.6 M
Total	**222**	**$12.7 M**	**$17.6 M**	**$38.2 M**	**$1.2 M**

Source: IMPLAN, RTI analysis of FY 2023 CCI spending data.
Note: Columns may not sum due to rounding.

Chapter 6

Financial Report

6.1 CCI Hub

The budget and expenditures for the CCI Hub in FY23 are shown in Figure 6.1.

The CCI Hub budget remained unchanged from FY22 at $7.5M to execute CCI's three mission lines: Research, Workforce Development, and Innovation. FY23 was a year of expansion and acceleration, particularly in the workforce development and innovation mission lines. CCI hired two research faculty and one Post-doctoral researcher and 24 part-time graduate research assistants to support specific grant research projects and testbed operations and maintenance.

In the workforce development and innovation mission lines, CCI initiated the "Friends of CCI" program to raise awareness of CCI's innovation and workforce development plans and programs among state and industry stakeholders. The "MeetUp2StartUp" program is an on-site networking opportunity that connects students and faculty interested in entrepreneurship with local, regional, or state-wide industry partners and/or venture capitalists to discuss commercialization ideas and hear from experts on market needs and best practices. CCI partnered with CACI to fund 11 project-based learning projects with students from the Northern Virginia Community College. The semester-long project provides the students with a CACI-developed project, along with CACI mentors, to work on a "real-world" project enabling the students to gain work experience to support future employment opportunities.

In the research mission line, CCI awarded eight grants for a network-wide research program, Securing Interactions between Humans and Machines. The evolution of artificial intelligence, cyber-physical systems, and communications is leading to a world in which humans and autonomous machines increasingly interact. In CCI, we view cybersecurity as intrinsically cross-disciplinary and devise solutions that lead to secure, resilient, and harmonious interactions between people and robots, drones, autonomous vehicles, and other cyber-physical systems. The CCI xG Testbed continues to gain national attention as one of the few end-to-end ORAN-compliant testbeds in the country. In FY23, the testbed was designated as an Open Test and Integration Center (OTIC) by the O-RAN Alliance. The O-RAN Alliance qualifies an institution as an OTIC only upon a thorough review involving technical capabilities, expertise, and community support, including partnerships with industry. An OTIC qualification is a sign of externally recognized worldwide excellence in O-RAN.

In FY23, CCI hosted the VASEM Annual Summit in Washington DC, and the second annual CCI Symposium in Richmond, VA. The VASEM Summit was a focused one-day event on the future security of cyberspace and its impact on the commonwealth and the Symposium is an opportunity for CCI researchers and students to discuss ongoing research projects, present posters on student research projects, and hear from cyber experts on current trends and opportunities in the cybersecurity research sector.

6.2 CCI Nodes

In FY23, 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 FY23, 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 FY23 are shown in Figure 6.2.

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.

Funds to support research are needed in four 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. Regarding continued funding of research scientists, funds are needed 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 will also be used to continue the support of an IT Engineer to manage the research projects associated with COVA SHARE. A total of $750,000 is allocated for research projects that are focused on cybersecurity in the Maritime environment. The cluster hire funds will be used to build an inter-institutional research center leveraging the strengths of ODU and GMU.

Funds to support regional innovation and development of the talent pipeline will be used to promote experiential learning, support undergraduate research, promote student-led innovation programs, continue to provide experiential learning programming for graduate students, support cybersecurity internships, support commercialization, and plan and support a cybersecurity workforce development conference and training, and continue to develop the CoVA CCI Regional Student 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. Funds to support a cybersecurity research and education conference are provided. The commercialization support in the upcoming year will be used to support the commercialization of previously funded CoVA CCI research.

6.2.2 Central Virginia Node

The budget and expenditures for the CVN in FY23 are shown in Figure 6.3.

In FY23, CVN continued to support all three CCI mission items, particularly focusing on Smart City Technologies and Medical Device Security. In the Workforce Development and Innovations mission line, CVN supported 15 projects: five from a CVN internal Experiential Learning Call for Proposals, five from a VCU internal Innovation Call for Proposals, and five from a UVA internal Innovation Call for Proposals.

In the Research mission line, CVN used funding to support existing programs at VCU and UVA. VCU continued to support ongoing CVN projects including the Smart City Testbed, Medical Device Security Testbed, and related ongoing research. CVN continued to support programs at UVA in research, workforce, and innovation programs that showed the best potential for impact as well as identify new opportunities focused on collaborating with partners within the CCI Central Virginia Node.

6.2.3 Northern Virginia Node

The budget and expenditures for the NoVA Node in FY23 are shown in Figure 6.4.

In FY22 and FY23, CCI NoVa Node made major investments in cybersecurity workforce development, attacking the challenge from every potential entry point and through novel modes of training and partnership. NoVa Node also made significant investments in the development of the cybersecurity innovation ecosystem through the establishment of the CATAPULT 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 have 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 CCI NoVa Node to enter FY23 with the ability to scale its success and impact.

In FY23, CCI NoVa Node made a significant number of faculty hires. To date, CCI NoVa Node has focused on issuing calls for proposals to seed research in key areas of interest to NoVa Node including cybersecurity as it relates to national defense, infrastructure, transportation, electric/power distribution, manufacturing sectors and resilience of cyber systems to human behavior. 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. The pivot from leveraging CCI dollars to fund NoVa faculty to the investment in new faculty, to collaborate across the Node and Commonwealth in order to compete for new external funding is expected to scale the impact of the CCI research endeavor. To seed the endeavor, CCI NoVa Node will hold one open call for research proposals in FY23 with focus 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.

In FY24, the CCI NoVa Node will continue 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 enable students to apply classroom knowledge to real world challenges and bridge the "experience" divide. These investments will widen the pipeline of cybersecurity career ready talent. In addition, the NoVa Node will continue to support each of its program participants to complete the George Mason University Clearance Readiness Program to expand the number of students across the NoVa Node who are prepared to enter and complete the security clearance process and denote that preparation with an electronic badge so employers can quickly identify these candidates. The most significant investment will be in subsidized internships. Investment will also be made to upskill non-degree seeking candidates, with special emphasis on displaced workers as a result of the pandemic, career changers, and those without prior cybersecurity training in order to widen the pipeline. NoVa Node will also support undergraduate research assistantships that enable undergraduates to participate in cybersecurity research enterprise and prepare them for work in established or emerging companies working at the leading edge of R&D. Finally, the NoVa Node will invest 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 will seek to expand the diversity of the cybersecurity workforce. CCI NoVa Node will also continue to build and expand the cybersecurity innovation and entrepreneur ecosystem in Northern Virginia and across the Commonwealth. In FY23, NoVa Node will expand its investment in Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology (CATAPULT) Fund to advance collaborative translational research projects among CCI partners, with the goal of speeding the transition of academic research outcomes to the marketplace. A key part of the success of CATAPULT has been 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 FY23, CCI+A plans to add an additional cohort of new companies. In addition to investment in the CCI+A, NoVa Node

will continue to support the successful Innovation Commercialization Assistance Program (ICAP) program which is developing new cybersecurity companies as they move through the customer discovery phase. ICAP serves as a feeder for CCI+A and together they are building the new cybersecurity innovation ecosystem in Virginia.

6.2.4 Southwest Virginia Node

The budget and expenditures for the SWVA Node in FY23 are shown in Figure 6.5.

The Southwest Virginia Node of the Commonwealth Cyber Initiative (CCI SWVA) continued to provide alignment of efforts in cyber research, innovation, and workforce development across a variety of stakeholders to demonstrate efficiencies and economies of scale. CCI SWVA partners coupled cores of technical excellence in wireless communications, emerging technologies, and cybersecurity with unique and expansive capabilities in the application domains of transportation, power systems, manufacturing, and agriculture, to discover, demonstrate, and commercialize technological solutions that will enable the next industrial revolution.

CCI SWVA continued major research initiatives in: Securing Time Synchronization and Applications to 5G/Next-G; Cryptography -Secure, distributed computing and communication; 5G Power Grid -Learning the Attackers' Behavior for Defense of Smart Power Infrastructures; Security and Privacy Aware Testbed for Voice-based Social Networks; High Accuracy Automatic Code Repair for Mission-critical Software; Space -Distributed Space Adaptive Communications and Security for Multi-Constellation Networks; and Quantum-Quantum Keys Management for Satellite Communications and Resurrecting SIKE: Developing and Implementing New Isogeny-Based Post-Quantum Schemes. The research mission of CCI SWVA was advanced through its Research Engagement, Seed Funding and Social Cybersecurity investments. The Research Engagement program included two tracks that gave opportunities for faculty to engage with startups or to perform work that would fund work to be able to propose to a much larger research opportunity. We funded twelve Research Engagement projects. Our Seed Funding program included projects that were submitted to the Research program that seemed promising but were not fully funded. We funded two additional projects from the Securing Interactions between Humans and Machines Call for proposals.

CCI SWVA continued its Regional Innovation thrust by providing support for our Innovation: Ideation to Commercialization program by funding 7 projects including: Anti-Counterfeiting Authentication App Using Deep-Learning-Based Physically Unclonable Functions; Cyber RADaR (Cybersecurity Rapid Asymmetric Discovery and Reporting) Phase Two: Commercially Deployed Beta Product and IP Registration; Power system reLiAnt Technology for Massive INterconnection of Integrated ReNEwables (PLATFORM-9); Protecting Bystander Visual Data Privacy in Augmented Reality Systems; Scalable Continuous Monitoring Solutions for Enterprise Security. We funded The Student Entrepreneurial Ideation Challenge (SEIC) that asked student teams from higher education institutions to team up to respond to an industry challenge. We also created the Cyber Innovation Scholar program that included a group of 24 doctoral candidates, master's students, and postdoctoral researchers who attended the first ever Cyber Startup Lab where they were introduced to processes involved in commercializing cyber technology.

CCI SWVA continued its Workforce Development thrust by investing in Workforce programs such as: Enhancing Cryptography Education Using Collaborative Visual Programming: A workforce development approach; HBCU Quantum Partnership Workshop; Pathways for Cyberbiosecurity Workforce Preparation: Integrating Insights from Both Cybersecurity and Biosecurity; Resilient and Secure BattleDrones: Drone Racing League for Southwestern Virginia; Broadening Participation in Security; and Women in Security. Other funded Workforce initiatives included a security readiness program, an Undergraduate Research program that allowed Radford students to participate in a research project at Virginia Tech and sponsorship of teachers to attend the Virginia Cybersecurity E education Conference. The CCI SWVA node also supported internship programs. We funded internships at the CCI SWVA Node, at the Virginia Cyber Range, at the Virginia Tech Information Technology area, at two leading industry partners, at VMI, at the Global Center for Automotive Performance Simulation organization, and through a Technology Enabled Internship and Mentoring program.

6.3 Geographic distribution of the awards from funds contained in HB30

Figure 6.6 shows the distribution of awards from funds in HB30.

CCI Hub Fiscal Year 2023		
FY23 Appropriation: $7,500,000		
Mission	Committed	Expenditure
Operations		
Labor (Faculty & Staff)		$ 3,421,341.00
IT/Phone/Print/Shipping	$ 2,879.00	$ 87,582.00
Supplies	$ 1,066.00	$ 14,861.00
Catering & Visitor Support		$ 6,609.00
Communications	$ 1,395.00	$ 15,373.00
Travel/Conferences/Workshops	$ 7,351.00	$ 75,325.00
CCI Symposium		$ 92,265.00
HR		$ 1,830.00
Operations/Rent/RTI Contracts	$ 48,482.00	$ 535,607.00
Sub Total	$ 61,173.00	$ 4,250,793.00
Workforce Development and Innovation		
Sub Awards (Programs)		$ 739,370.00
Meet Up to Startup		$ 1,746.00
Sponsorships		$ 5,600.00
Program Management		$ 1,119.00
Camps/Internship Fair/Cyber Fusion		$ 29,789.00
CATAPULT Co-Sponsorship		$ 200,000.00
Sub Total	$ -	$ 977,624.00
Research		
Hub Sponsored Research Projects		$ 697,000.00
Hub Sponsored Network Programs	$ 170,000.00	$ 300,000.00
xG Testbed	$ 66,536.00	$ 128,947.00
xG Testbed Contract Support		$ 100,121.00
ECE Graduate Student Funding		$ 603,988.00
GRA Tuition		$ 61,504.00
Professional Development		$ 9,081.00
Mobile World Congress		$ 39,596.00
Supplies/Equipment		$ 33,934.00
Sub Total	$ 236,536.00	$ 1,974,171.00
Totals	$ 297,709.00	$ 7,202,588.00
Total Expenditure & Committed		$ 7,500,297.00

Figure 6.1: Budget and expenditures for CCI Hub in FY23.

CCI Coastal Virginia Node Fiscal Year 2023	
FY23 Appropriation: 2,500,000	
Mission	**Expenditure**
Operations	
Personnel Costs	245,409
Other Operating Costs	61,771
Sub Total	**307,180**
Workforce Development and Innovation	
Experiential Learning Admin Support	5,000
Undergraduate Research Program	98,000
Innovate Cyber Challenge	105,446
Graduate Student Experiential Learning	102,627
Cybersecurity Regional Student Assoc	18,054
Workforce Dev Training / Conference	24,322
CODE Va / CyberStart America	15,000
Sub Total	**368,449**
Research	
Research FTEs (Salary & Fringe)	908,486
CCI Fellows-Research Scientist Hires	220,000
COVA SHARE (Research lab)	12,267
COVA SHARE (SEIM Lifecycle Replace)	75,000
Maritime Research Projects	581,014
Doctoral Fellowships	50,000
Sub Total	**1,846,767**
Total Expenditure	**2,522,396**

Figure 6.2: Budget and expenditures for the CoVA Node in FY23.

CCI Central Virginia Node Fiscal Year 2023	
FY23 Appropriation: 2,500,000	
Mission	Expenditure
Operations	
Personnel	280,000
CVN Operations	50,000
CVN Partner Institutions	120,000
Community Outreach/Events	50,000
Sub Total	**500,000**
Workforce Development and Innovation	
Experiential Learning CFP	150,000
Internships in CVN	150,000
Innovation in CVN	200,000
Sub Total	**500,000**
Research	
Support Existing Programs	450,000
Research Faculty	250,000
Research CFP's	800,000
Sub Total	**1,500,000**
Total Expenditure	**2,500,000**

Figure 6.3: Budget and expenditures for the CVN Node in FY23.

CCI Northern Virginia Node Fiscal Year 2023	
FY23 Appropriation: 2,500,000	
Mission	Expenditure
Operations	
Admin/Operations	220,000
Sub Total	**220,000**
Workforce Development and Innovation	
Undergraduate Research Assistants	80,000
Cybersecurity Apprenticeship	400,000
Undergraduate Internships	100,000
Cyber.org Teacher Program	30,000
High School Internships	120,000
CCI+A (CATAPULT)	250,000
ICAP	100,000
Sub Total	**1,080,000**
Research	
Securing Interactions CFP	200,000
Faculty Hires	1,000,000
Sub Total	**1,200,000**
Total Expenditure	**2,500,000**

Figure 6.4: Budget and expenditures for the NoVA Node in FY23.

CCI Southwest Virginia Node Fiscal Year 2023	
FY23 Appropriation: 2,500,000	
Mission	Expenditure
Operations	
Personnel	289,040
Other Operations Costs	11,723
Sub Total	**300,763**
Workforce Development and Innovation	
Innovation Programs	382,750
Workforce Programs	338,943
Sub Total	**721,693**
Research	
Major Research Programs	1,013,453
Seed Funding Program	120,000
Research Engagement Program	260,000
Faculty Hire	84,091
Sub Total	**1,477,544**
Total Expenditure	**2,500,000**

Figure 6.5: Budget and expenditures for the SWVA Node in FY23.

Geographic Distribution of Awards from the Funds Contained in HB30

Node	Number of Awards	Grant Total
Central Virginia	9	$3,005,000
Coastal Virginia	6	$2,944,370
Northern Virginia	8	$2,851,660
Southwest Virginia	9	$3,028,334
Total	**32**	**$11,829,364**

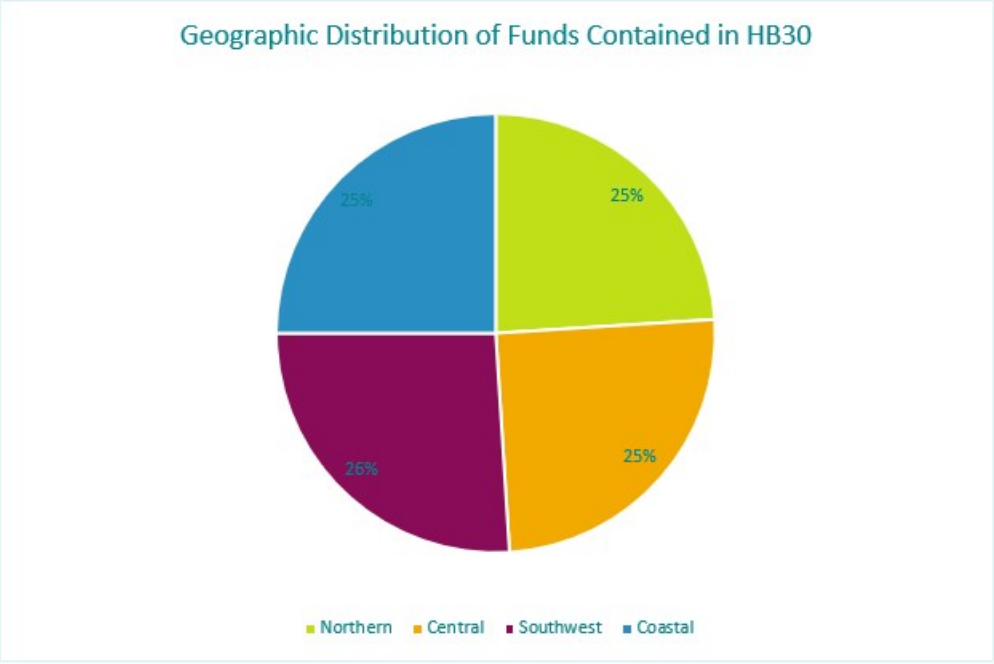


Figure 6.6: Geographic distribution of awards using FY23 funds.

Chapter 7

Looking Ahead: FY24

In FY23 we continued to invest in innovation and workforce development programs launched by the CCI Hub and by each of the regional Nodes. We also saw a huge increase in extramural funding for CCI researchers. Most of this report thus far has been devoted to describing the main accomplishments of the CCI network in FY23. In this chapter, we outline the main activities and programs planned for FY24.

Our major goals for the coming fiscal year include:

- Continued focus on large-scale, multi-institutional research grants.
- Engagement with industry through a new NSF industry-university center.
- Capacity building in supply chain security.
- Leadership in open radio access networks.
- Expansion of international engagement.
- Continued investment in experiential learning.
- New and continuing innovation programs.
- Development of a strategic plan for the next seven years.

We discuss each of these goals in turn.

7.1 Focus on large-scale, multi-institutional research grants

We will continue to fund CCI Fellows committed to leading center-scale grants involving more than one CCI institution. This strategy is already giving impressive returns: the 115% increase in extramural funding in FY23 is largely due to a large number of new large research contracts. Former CCI Fellows Jack Davison, Duminda Wijesekera, and Sachin Shetty led some of the $1M+ grants received by CCI from federal government sources in the past.

We have funded six new CCI Fellows in FY23. They have committed to leading large research proposals to be submitted in FY24 on the following topics:

- Mohamed Azab, assistant professor of computer and information sciences at Virginia Military Institute, is leading a Cybersecurity-Aware Workforce Development Platform for Mission Critical Applications proposal.
- Jonathan Black, Professor in the Kevin T. Crofton Department of Aerospace and Ocean Engineering at Virginia Tech, is leading a Center for Secure Space Communications proposal.

- Returning Fellow Jack Davidson, professor of computer science in the School of Engineering and Applied Science and director of the Cyber Defense program of study at the University of Virginia, is leading a Building a Commonwealth Community Scientific Instrument to Support Data-driven Cybersecurity Research project.
- Jonathan Goodall, professor in the Department of Civil and Environmental Engineering at UVA and Director of the UVA Engineering LINK LAB, is leading a Smart Cities Technologies for Coastal Resilience proposal.
- Parth Pathak, associate professor in the Computer Science Department at George Mason University, is leading an Open-Milli-IoT: An Open Programmable Platform for mmWave Wireless Internet-of-Things project.
- Aidong Zhang, Thomas M. Linville Professor of Computer Science at the University of Virginia, is leading an Intelligent Ambient Computing in Dynamic Environments proposal.

7.2 Engagement with industry through a new NSF industry-university center

A CCI team lead by Dr. Luiz DaSilva will submit 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 four CCI universities, ODU, VCU, VT, and Mason, as well as the University of Arizona.

The submission is a revised version of a proposal submitted to NSF in December 2022, which was recommended for funding by the review panel but ultimately not funded. If successful, 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. Our previous submission included letters of financial commitment from 24 industry partners willing to commit an average of $50K in funding per year to the center.

The proposed Center for Wireless Innovation towards Secure, Pervasive, Efficient and Resilient Next Generation Networks (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 precompetitive 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.

The proposed WISPER Center will contribute significantly to the country's future communication infrastructure, with broader impacts on diversity and inclusion, workforce development, and technology transfer. A Diversity & Inclusion Committee will be formed to review the current diversity and inclusion profile and develop specific measures and plans for inspiring the participation of underrepresented groups. WISPER will 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 Capacity building in supply chain security

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 and 2021's securing the next generation of networks.

This year, we are looking for proposals that advance supply chain cybersecurity. The main objective is to identify, evaluate, and mitigate risks that arise when working with third parties in the supply chain. Supply chain cybersecurity applies to software, services, and products.

Potential topics include but are not limited to:

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

7.4 Leadership in open radio access networks

The development of Open Radio Access Network (O-RAN) is an important priority for the U.S., with $1.5 billion appropriated for the development of wireless innovation under the CHIPS and Science Act. Success in that area 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.

The CCI xG Testbed now boasts the only Open Testing and Integration Center (OTIC) in the Commonwealth of Virginia and the Washington, D.C., region. One of six centers in North America and one of 15 in the world approved by the O-RAN Alliance, the CCI center will be an essential component to boosting advancements and competition in wireless mobile networks based on open radio interfaces.

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.

CCI received the OTIC designation due to its xG Testbed, the first end-to-end O-RAN-compliant testbed of its kind in the United States. Based at the Virginia Tech Research Center in Arlington, the testbed will serve as the OTIC host in partnership with AT&T, DISH Network, and Verizon. CCI partners — George Mason University, Wireless@VT, and Old Dominion University — are also involved, working together toward the goal of accelerating O-RAN advancement, innovation, and deployment.

In addition to the testbed in Arlington, an outdoor campus-scale testbed is under construction on Virginia Tech's Blacksburg campus. Its features include three commercial Citizens Broadband Radio Service (CBRS) base stations.

The next generation of communication networks has changed the traditional monolithic hardware base station to a disaggregated and virtualized base station, using mostly software instead of hardware to get the job done. Base stations have three components — a centralized unit and a distributed unit, which are both software driven, and the physical radio unit or antenna. Different companies may build each separate component. Ensuring these different components work seamlessly together and spotting opportunities for improvement is where OTIC and the CCI xG Testbed can provide essential expertise.

OTICs are vendor-independent and designed to encourage and enable wide adoption of O-RAN specifications by confirming equipment manufacturers, system integrators, and software providers follow O-RAN Alliance guidelines. With a common platform and processes, OTICs can allow manufacturers to speed development of new radio access network technologies and products.

7.5 Expansion of international engagement

Our vision, as stated in Chapter 1, is to establish Virginia as a *global center of excellence* in cybersecurity. One of the goals for FY24 is to significantly expand our international presence.

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.
- Plan the first international CCI workshop, to build research and innovation partnership between CCI researchers and some of the top institutions in Europe and Asia.

7.6 Continued investment in experiential learning

Our internship and apprenticeship programs have been among the most successful experiential learning programs that CCI has created. They have attracted an extremely diverse population of students, a particular victory in cybersecurity, where women, Black, and Latino professionals are still severely underrepresented. These programs are also heavily oversubscribed, and we are able to only select a small portion of the applicants for funding.

The demand for these programs confirms that they fill an important need: practical experience is critical for retention of students in cybersecurity and in these students' competitiveness for good jobs once they graduate.

In FY24, the CCI Hub and Nodes will continue to invest in programs that provide students with hands-on experience, working closely with their future employers. For the fifth consecutive year, we will run a call for internal CCI proposals in experiential learning in Spring 2024. Some of the most successful workforce development programs in CCI had their start through those calls. Over the years, the terms of funding have evolved, and we now require that the programs be partially funded by industry or government partners.

We will also continue to build programs tailored to the needs of particular partners. A blueprint for this type of program is the project-based learning program described in Section 3.1.3, currently being piloted with students in NVCC. In FY24, this program will be expanded to other community colleges in the commonwealth.

7.7 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 FY24, there are Meet Up to Startup events already scheduled for: Harrisonburg, hosted by James Madison University (JMU); Charlottesville, hosted by UVA; Fairfax, hosted by Mason; Williamsburg, hosted by W&M; and Lexington, hosted by VMI. Venture Capitalists attending include: VTC Ventures, Paladin Capital Group, Shenandoah Community Capital Fund, DREAMIT VENTURES, and Rocktown Angels.

The CCI Hub and NoVA Node will again 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.

We also continue to have monthly 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.

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

In FY24, we will release CCI 2030, a strategic plan for the next seven years. The development of the plan is being led by the CCI Hub in close partnership with the Leadership Council and the CCI Inclusion and Diversity Committee. A survey has been distributed to the entire CCI network of researchers, providing an opportunity for input from a broad array of stakeholders. CCI's TAB will provide 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.

Appendices

CCI Extramural Funding for FY23
Appendix 1

CCI Hub

Project Title	Lead Institution	Funding Amount	Funding Agency
Automated Cyber-Attack Detection and Mitigation under Non-Stationary using Operating Envelopes	Virginia Tech	$112,836	NSA
Graduate Student Research Program on Artificial Intelligence Enabled Technologies	Virginia Tech	$150,000	Deloitte & Touche
IUCRC Planning Grant	Virginia Tech	$20,000	NSF
Open-Milli-IoT: An Open Programmable Platform for mmWave Wireless Internet of Things	Virginia Tech	$50,000	
ATIS Next-G Alliance Renewal	Virginia Tech	$212,674	VT-ARC
NSF Convergence Accelerator Track G	Virginia Tech	$80,000	NSF
SWIFT: Context Aware Spectrum Coexistence Design and Implementation in Satellite Bands	Virginia Tech	$173,167	NSF
ATIS Next G Alliance Renewal Part 2	Virginia Tech	$134,133	VT-ARC
Deep Reinforcement Learning Enabled Warfighter Assistance (DICE)	Virginia Tech	$45,001	Missile Defense Agency
Total		**$977,811**	

CCI Extramural Funding for FY23
Coastal Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
HRBRC collaboration Accelerator Fund, "Social Estrangement and Virtual Connectivity of Children in COVID Era"	NSU	$150,000	HRBRC
Learning based Dynamic Spectrum Sharing for NextG Networks	ODU	$250,000	Department of the Army
Distributed Secure Live, Virtual, and Constructive (LVC) Air Combat System Training Environment (SLATE)	ODU	$170,000	DoD
Collaborative Research: CISE-MSI: DP: CNS: Efficient Data Communication and Processing for Intelligent Medical Systems with Edge-Cloud Interplay	ODU	$360,000	NSF
Cyber Risk and Resilience Analytics	ODU	$654,358	Frontier Technology Inc.
Center of Excellence in Machine Learning	ODU	$350,000	DoD
Mission Analytics for Electronic Warfare by quantifying impact of RF-enabled Cyber attacks	ODU	$100,000	U.S Navy (NSWC)
Joint Semi-supervised conditional random field and graph attention network for power grid collateral damage	ODU	$22,500	AFRL
CyberCorps Scholarship for Service: Preparing Future Cybersecurity LeADERS through applied learning experiences	ODU	$1,037,432	NSF
Supplemental Bridge Grant for CyberCorps Scholarship for Service: Preparing Future Cybersecurity LeADERS through applied learning experiences	ODU	$116,380	NSF

CCI Extramural Funding for FY23
Coastal Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Visiting Faculty Research Program Award at Air Force Research Lab, "Physics-informed image processing for battlefield building damage image processing"	ODU	$18,757	AFRL
Visiting Faculty Research Program Extension Award, "Learning a Hierarchical Multi-scale Generative Adversarial Network for Building Damage Estimation and Disaster Recovery using Remote Sensing Images"	ODU	$10,000	AFRL
Visiting Faculty Research Program Extension Award, "Learning a Hierarchical Multi-scale Generative Adversarial Network for Building Damage Estimation and Disaster Recovery using Remote Sensing Images"	ODU	$22,464	AFRL
Naval Station Norfolk 5G Enhanced Infrastructure and Applications Prototype	ODU	$138,432	Booz, Allen, Hamilton
Advanced Machine Learning Artificial Intelligence	ODU	$345,000	Applied Research LLC
Pursuing Interoperability in Utilitarian Online Learning Models	ODU	$175,000	NSF
Facilitate the Convergence of the Next Gen AI and Wireless	ODU	$100,000	Interdigital Co
Blockchain based AI/ML Management to Enable Multi-modal Federated Learning	ODU	$100,000	Interdigital Co.
Smart Grid Digital Twin Based on Physics-informed Reinforcement Learning Model	ODU	$1,500,000	Department of Education
ODU/NNPS College Partnership Laboratory School Planning Grant	ODU	$200,000	Virginia DoE
ODU/CPS College Partnership Laboratory School Planning Grant	ODU	$200,000	Virginia DoE
Go VA: Greater Opportunities in Tech	ILAR	$463,017	Go VA
Total		**$6,366,960**	

CCI Extramural Funding for FY23
Northern Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
CRII: CNS: Security Assessment	George Mason	$134,706	NSF
ArtlAMAS 2.12	George Mason	$118,694	UMD
CollabRes: SaTC: CORE Med: Infrastructure	George Mason	$600,000	NSF
CollabRes: SaTC: CORE Med: Infrastructure	George Mason	$16,000	NSF
Coll Res: Accelerator Design	George Mason	$195,362	NSF
CollabRes: SaTC: CORE: Med: EcryptDB	George Mason	$114,466	NSF
Risk Prediction IT	George Mason	$254,614	NSF
DASS: SS Provisioning System	George Mason	$153,440	ASU/NSF
Mapping Info Ecology	George Mason	$149,921	ASU/NSF
IUCRC Planning: WISPER	George Mason	$20,000	NSF
CNS: Core: Small NV-RGRA	George Mason	$309,261	NSF
EAGER: Inclusive Scam Detection	George Mason	$299,248	NSF
Seed Grant	George Mason	$995,256	ORIEI
Integrated Photonics	George Mason	$900,000	NCMS/DoD
ARLIS Support	George Mason	$100,000	UMD/IARPA
Study	George Mason	$1,500,000	CDAO
Pilot	George Mason	$1,500,000	CDAO
Immersion Teams	George Mason	$866,250	CDAO
GIDE Clinics	George Mason	$29,252,000	CDAI
CollabRes: RI: CCRI: New Space	George Mason	$299,989	NSF
5G-IPS Firefighters using UAVs	George Mason	$1,199,950	NIST
2022 NCAE	George Mason	$500,000	NSA
Auto Security Patch Generation	George Mason	$212,000	ONR
CR: SWIFT IDEA	George Mason	$300,000	NSF
CCSS: Distributed Swarm Learning	George Mason	$400,000	NSF
Connected Room	George Mason	$50,009	Private Sector Company
Serverless Architecture	George Mason	$49,742	Private Sector Company

CCI Extramural Funding for FY23
Northern Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
5G Tech and Edge Security	George Mason	$50,009	Private Sector Company
InfoSec Assessment	George Mason	$75,000	Private Sector Company
TrackG: Secure Texting in 5G	George Mason	$750,000	NSF
Wave Communications	George Mason	$1,000,000	USN
Cyber Infrastructure: ITProgram	George Mason	$926,000	USED
Cyber Infrastructure: ITProgram	George Mason	$74,000	USED
CollabRes: CNSCore: Med: VidStream	George Mason	$196,781	NSF
CollabRes: CNSCore: Med: VidStream	George Mason	$16,000	NSF
Enabling Zero Trust Authentication for Metaverse	George Mason	$98,185	Cisco Systems
Total		**$43,676,883**	

CCI Extramural Funding for FY23
Central Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
OCC Development	Virginia Commonwealth	$25,000	Micron
Quantum Entangled SWIR Photon Source	Virginia Commonwealth	$416,000	U.S. Air Force
Army Strategic Program for Innovation and Employment (ASPIRE)	Virginia Commonwealth	$275,000	U.S. Army
Thin Meta-structure Enhanced Near Room Temperature MWIR Detectors Air Force Science for Minority Advancement, Research and Training (Å-SMART)	Virginia Commonwealth	$245,000	U.S. Air Force
Dual Integrated Soliton Computation System (DISCS)	Virginia Commonwealth	$500,000	DARPA
Focused CoPe: Enhancing Resilience and Equity in Urban Coastal Communities through the Co-Generation of Community Capitals	University of Virginia	$5,000,000	NSF
SCH: INT: Context-Aware Micro-Interventions for Social Anxiety	University of Virginia	$1,500,000	National Institutes of Mental health
Collaborative Research: Research Initiation: Formation of the Foundations for Engineering Intuition in Structural Engineering with Mixed Reality	University of Virginia	$200,000	NSF
Total		**$8,161,000**	

CCI Extramural Funding for FY23
Southwest Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Murder Mystery to Promote Learning of Structured Query Language (SQL)	Virginia Tech	$20,000	4-VA
Distributed Heterogeneous Space Communications Testbeds	Virginia Tech	$80,000	NGI Atlantic
Distributed Space Adaptive and Assured Communications and Security for Multi Constellation Networks	Virginia Tech	$100,000	Peraton
Modeling Bundle Routing Protocols for Use within Space mesh Network Simulation Scenarios	Virginia Tech	$100,000	Peraton
Measuring and Auditing Route Origin Validation (ROV) of Network Operators for RPKI	Virginia Tech	$75,000	Comcast Innovation Fund
Collaborative Research: Research Infrastructure: CCRI: New: Distributed Space and Terrestrial Networking Infrastructure for Multi-Constellation Coexistence	Virginia Tech	$1,699,997	NSF
QuIC-TAQS: Quantum Networking with Multipartite Entangled Photons	Virginia Tech	$400,000	NSF
Platform-Agnostic Privacy Leakage Monitoring for Machine Learning Models	Virginia Tech	$98,372	Amazon
Enabling High-Fidelity Cyber Threat Knowledge Acquisition from Open-Source Cyber Threat Intelligence	Virginia Tech	$15,000	4-VA
Collaborative Research: SaTC: CORE: Medium: An Anti-tracking and Robocall-free Architecture for Next-G Mobile Networks	Virginia Tech	$600,000	NSF

CCI Extramural Funding for FY23
Southwest Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Collaborative Research: SaTC: CORE: Medium: A Networking Perspective of Blockchain Security: Modeling, Analysis, and Defense	Virginia Tech	$600,000	NSF
Physics-aware AI-based Approach for Cyber Intrusion Detection in Substation Automation Systems	Virginia Tech	$250,000	C3AI
Development of IDS Algorithm for Ensemble Cyber Security Model	Virginia Tech	$300,000	NREL
Cyber Resilience of Substations (CREST) for Grid Operation and Control	Virginia Tech	$1,964,000	DoE
5G Technology Platform for Military Bases with a Resilient, Green, And Secure Electric Grid (5G BASE)	Virginia Tech	$50,000	U.S. Army Corps of Engineers
Physics-Aware AI Based Approach to Cyber Intrusion Detection in Substation Automation Systems	Virginia Tech	$120,000	University of California-Berkley
Evaluation codes, duals, and applications	Virginia Tech	$568,830	NSF
Secure and Trustworthy Data and Technology: Evolution to a New Era	Virginia Tech	$25,000	4-VA
Collaborative Research: Evaluation Codes, Duals, and Applications Research Experiences for Undergraduates (REU) supplement	Virginia Tech	$57,300	NSF
Collaborative Research: Evaluation Codes, Duals, and Applications Research Experiences for Teachers (RET) supplement	Virginia Tech	$35,000	NSF
5G Technology Platform for Military Bases with a Resilient, Green, And Secure Electric Grid (5G-BASE)	Virginia Tech	$40,000	U.S. Army Corps of Engineers

CCI Extramural Funding for FY23
Southwest Virginia Node

Project Title	Lead Institution	Funding Amount	Funding Agency
Scalable Secure coordinated Connectivity for Renewable DERs in power Grid (SECURED-GRID)	Virginia Tech	$800,000	DoD
NSF CPS Cybersecurity of the distribution system (CYDER) INTERN	Virginia Tech	$55,000	NSF
NEC 5G Deployment and 5G Implementation (Phase 2)	Virginia Tech	$143,000	NEC (Private)
Registered Apprenticeship Program	Radford University	$8,100	DoL/CTE
5G-based Indoor Positioning System for Firefighters using UAVs	Virginia Tech	$1,199,950	NIST
VSU Partnership Development	Virginia Tech	$750,000	Genentech Foundation
VSU Partnership Development	Virginia Tech	$75,000	Sloan Foundation
ACCOLADE	Virginia Tech	$300,000	DoD
SMC 2023	Virginia Tech	$3,206,999	NSA
GenCyber Capacity Grant	Virginia Tech	$100,000	GenCyber NSA
SaTC: CORE: Small: Systematic Threat Characterization and Prevention in Open-Domain Dialog Systems	Virginia Tech	$600,000	NSF
CRDF Global RFP Submission_ Cybersecurity Expertise	Virginia Tech	$24,072	CRDF Global
DSFAS: Audio data as a novel trait to manage welfare and environmental impact in precision cow farming	Virginia Tech	$649,761	USDA NIFA
Privacy-Preserving Computation in Heterogeneous Architecture with Minimal Trust	Virginia Tech	$750,000	AFOSR
Combating Insider Threat: Identification, Monitoring, and Data	Virginia Tech	$99,545	Cisco
Total		**$15,959,926**	

Securing Interactions Between Humans and Machines Research Grants by Node
Appendix 2.2.1

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
SocialAssess – An Assessment Framework for 'Information-Handling' Practices on Social Media	Tamer Nadeem	Virginia Commonwealth University	Jeanine Guidry / Virginia Commonwealth University	$60,000
Biometrically Secure Human Robot Interaction	Kate Sicchio	Virginia Commonwealth University	Joseph Shelton / Virginia State University	$60,000
Attacking and Securing Algorithmic Fairness in Human Machine Interactions: A Cross-Disciplinary Framework	Jungdong Li	University of Virginia	Jess Reia / University of Virginia	$60,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
TrustAI: Enhancing Human Confidence and Trust in Deep Learning Models	Rui Ning	Old Dominion University	Xiao Yang / Lusi Li / Old Dominion University Xinwei Deng / Virginia Tech	$60,000
From Gap to Gain: Counter Human Smuggling by Identifying Deceptive Advertisements in Social Media	Faryaneh Poursardar	Old Dominion University	Vikas Ashok / Erika Frydenlund / Old Dominion University	$60,000

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Privacy-preserving Mapping and Localization for Immersive Healthcare Applications	Bo Han	George Mason University	Songqing Chen / Hong Xue / George mason University	$60,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Understanding the Impact of Data Privacy Regulations on Software and Its Stakeholders	Chris Brown	Virginia Tech	Aaron Brantly / Virginia Tech	$60,000
Assuring Trustworthy and Secure Human-AI Collaboration to Strengthen America's Civil Infrastructure: A Virtual Reality Prototype	Rodrigo Sarlo	Virginia Tech	Ismini Lourentzou / Feras Batarseh / Joe Gabbard / Virginia Tech Stephanie Blackmon / William & Mary	$60,000

SWVA Research Engagement Program
Appendix 2.2.2

Southwest Virginia Node Research Engagement Program

Project Title	PI	Lead Institution	Grant Amount
Distributed In-Network Authentication for Zero-Trust Security Enabled by Programmable Switches	Peng Gao	Virginia Tech	$20,000
Enhancements of SQISign	Jason LeGrow	Virginia Tech	$20,000
Inverters for Clean Holistic Electricity Security	Ali Sani-Mehrizi	Virginia Tech	$20,000
Manufacturing Engineering Education Program Research Engagement	Bradley Davis	Virginia Tech	$20,000
Novel Algebraic-Models for Resiliency Planning of Networked-Sensors and their Information Transmission Network from Cyber Attacks	Manish Bansal	Virginia Tech	$20,000
Proposal team Building and Privacy Expert Recruitment for a Workshop on Bystander Obscuration in Wearable Augmented Reality Displays	Alan Michaels	Virginia Tech	$20,000
Secure and Self-powered Wireless Internet of Things (IoT) Devices Through Physical Unclonable Functions and Energy Harvesting	Sook Ha	Virginia Tech	$20,000
SmartGuide: Revolutionizing the Depth and Dependability of Vision-Impaired Navigation	Luis Borunda Monsivais	Virginia Tech	$20,000
Supporting AI-Driven Clinical Applications: Novel Privacy-Preserving Training Methodology for Federated Learning on Sensitive Healthcare Data	Derek Kaknes	Virginia Tech	$20,000
Towards Open Knowledge Network Construction, Adaptation, and Deployment	Junjie Hu	Virginia Tech	$20,000
Trustworthy Multimodal Machine Learning in Healthcare: Aligning Model Attention with Human Attention	Aiguo Han	Virginia Tech	$20,000
Wireless Security with Data Oriented Modalities (WISDOM)	Tugba Erpek	Virginia Tech	$20,000
Total			**$260,000**

2023 CCI Cyber Arts & Design Research Grants by Node

Appendix 2.2.5

Central Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
SentimentVoice: Integrating emotion AI and VR in Performing Arts	Semi Ryu	Virginia Commonwealth University	Alberto Cano / Virginia Commonwealth University	$25,000

Coastal Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Unveiling Invisible Sight: Exploring AI Perception and Privacy in IoT Devices through Interactive Art	Rui Ning	Old Dominion University	Liuwan Zhu, PhD Student / Old Dominion University	$25,000

Northern Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Designing the Next-Generation Security Warnings to Mitigate Social Media Misinformation	Chen Guo	James Madison University	Nan Zheng / Chengqi Guo / James Madison University	$25,000
Cyber Insecurity: Exploring Vulnerabilities of Artificial Intelligence Through Visual Art	Marlena Jarboe	Blue Ridge Community College	Jennifer Whitmore / Daniel O'Brien / Harpeet Panesar / BRCC Jerome Sturm / VCCS	$25,000

Southwest Virginia Node

Project Title	PI	Lead Institution	Co-PIs & Institution	Grant Amount
Interactive theatre to increase cybersecurity preparedness and prevent scams targeting older people: a community-building interdisciplinary project.	Susanna Rinehart	Virginia Tech	Katalin Parti / Pamela Teaster / Virginia Tech	$25,000
Hidden Within	Agnieszka Miedlar	Virginia Tech	Janet Biggs / Paul Cazeaux / Tanner Upthegrove / Virginia Tech Daniel Takaki / University of Kansas	$25,000

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/