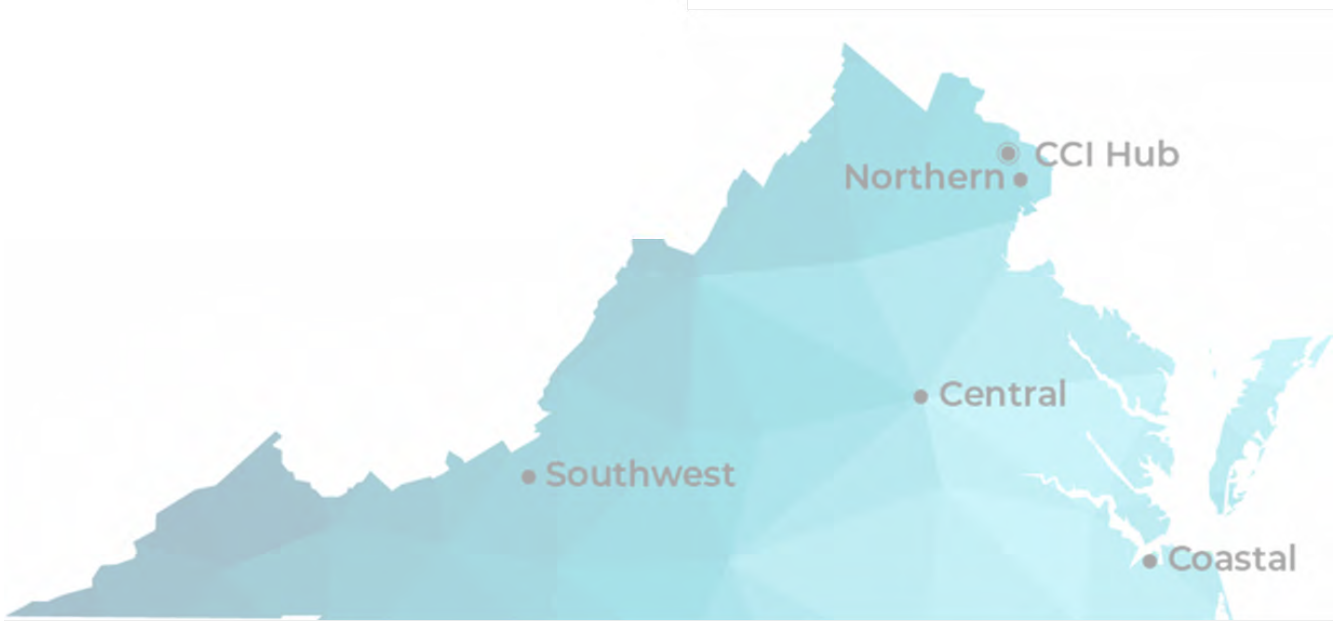
Commonwealth Cyber Initiative
COASTAL VIRGINIA

Coastal Virginia Center for Cyber Innovation (COVA CCI)

Annual Report July 2025 – June 2026



Research | Innovation | Workforce Development

July 31, 2026

Daniel Takabi – Director
John Costanzo – Chief Administrative Officer

Commonwealth Cyber Initiative
COASTAL VIRGINIA

Contents

Executive Summary ***4***
Chapter 1: COVA CCI Introduction ***6***
Chapter 2: Research Programs ***8***
Chapter 3: Workforce Development and Experiential Learning Programs ***17***
Chapter 4: Economic Impact/Innovation ***27***
Chapter 5: Collaborative Partnerships and Projects ***30***
Chapter 6: Financial Report ***31***
Chapter 7: Other COVA CCI Programs and Initiatives ***33***

Message from Dr. Daniel Takabi, COVA CCI Director

The Coastal Virginia Center for Cyber Innovation (COVA CCI) was established to catalyze cybersecurity research, bridge the gap between academic researchers and industry, and provide high0impact experiential learning opportunities to students in our region. As the regional node of the Commonwealth Cyber Initiative (CCI), COVA CCI's impact has far exceeded expectations. Through strategic investments including supporting 12 research faculty, supporting the William & Mary Cyber Policy and Law Group, funding 22 grants, and providing critical workforce development to over 700 students via internships and innovation training, COVA CCI has solidified its role as a vital engine for regional economic growth and innovation. Beyond these quantitative metrics, our true impact lies in the unprecedented depth and strength of the collaborative networks established among our partners

This annual report highlights COVA CCI's most notable milestone achievements. Over the past fiscal year, we expanded our portfolio with several forward-looking initiatives designed to deepen collaboration. These include launching the COVA CCI Researcher Symposium, issuing targeted research grants focused on Agentic AI Cybersecurity and Security for Agentic AI, co-hosting a high-profile Cyber Summit alongside the FBI Norfolk, and sponsoring the inaugural national CyberAI competition.

Building on this robust foundation, we remain committed to scaling our impact across the region. I am immensely proud of our cumulative progress in research excellence, technical innovation, and workforce readiness. As we review the accomplishments detailed in this report, we do so with a clear trajectory toward a highly successful and innovative future.

Commonwealth Cyber Initiative
COASTAL VIRGINIA

Executive Summary

Reporting Period: July 2025 – June 2026
Director: Dr. Daniel Takabi | Chief Administrative Officer: John Costanzo

---

The Coastal Virginia Center for Cyber Innovation (COVA CCI), Southeastern Virginia's regional node of the Commonwealth Cyber Initiative (CCI), continues to serve as a leader in cybersecurity research, workforce development, innovation, and industry partnerships across Southeastern Virginia. With a mission to advance cybersecurity, artificial intelligence (AI), and 5G, COVA CCI is creating a collaborative, talent-rich ecosystem to support Virginia's digital economy.

Strategic Focus and Regional Network

COVA CCI has built a strong regional network comprising over 100 researchers and faculty from 10 higher education institutions and more than 20 business and government partners. Partner organizations include CISCO, Deloitte, Sentara Healthcare, Huntington Ingalls Shipbuilding, the U.S. Navy, the City of Virginia Beach, and the City of Suffolk. In FY26, the center continued to emphasize cybersecurity research, AI integration, and the commercialization of cybersecurity solutions.

Research Achievements

COVA CCI supports multiple lines of effort in cybersecurity research, including work in AI and Machine Learning, Next G, Maritime and Supply Chain Cybersecurity, and others. We collaborate with a diverse range of researchers from various universities and public and private organizations.

- **External Grants**: COVA CCI researchers secured over $9,272,555 million in grant funding from federal, state, and private entities.
- **Internal Research**: Six (6) research projects were funded under the FY26 COVA CCI Cybersecurity Research Program totaling $479,926. These projects focused on Agentic AI Cybersecurity and Security for Agentic AI.
- **CCI & NOVA Node Collaboration**: Sixteen (16) additional projects were funded for a combined $1,304,962.
- **Research Faculty**: COVA CCI supported twelve (12) research scientists and one IT engineer across institutions, with new hires expanding capabilities in AI, maritime security, and quantum computing.
- **Shared Computing**: Continued development of the COVA SHARE collaborative research environment supported ongoing inter-institutional work.

Workforce Development and Experiential Learning

A cornerstone of COVA CCI's mission is to prepare the next generation of cybersecurity professionals through hands-on experience and research training. In FY26, 127 students participated in its programs:

- **Cybersecurity Undergraduate Research Program**: 31 students from 7 institutions engaged in publishable research projects. Since its inception, 167 students have completed the program.
- **Innovate Cyber Challenge**: 41 students from 6 universities tackled real-world cyber challenges using design thinking. The program supported 267 students.
- **Internships**: COVA CCI supported 13 interns with ODU's Center for Educational Innovation & Opportunity (CEIO), who supported multiple community STEM outreach events for K-12 students.
- **Cybersecurity Clinic**: 42 students worked with 10 clients, including the City of Suffolk and local businesses, offering no-cost cybersecurity services. Since its launch in spring 2024, the clinic engaged 83 students and 25 organizations.

Innovation and Economic Impact
COVA CCI emphasizes applied innovation and commercialization:

- Supported student entrepreneurs in developing cybersecurity-related products or services through the Innovate Cyber program and Undergraduate Research Program.

In 2025, CCI had an economic impact analysis completed that showed COVA CCI's annual economic output is approximately $10.3 million, supporting around 137 jobs and generating up to $1.1 million in state and local tax revenue.

Student Leadership and Outreach
COVA CCI supports and elevates student voices through the Coastal Virginia Cybersecurity Student Association (CVCSA), which:

- Hosted CyberForge 2026, drawing over 130 participants to its CTF and conference.
- Initiated the statewide Virginia Cybersecurity Students (VCyS) network, creating four regional student hubs for innovation and engagement.

Additionally, COVA CCI co-hosted events with William & Mary's Center for Legal & Court Technology, including a global symposium on Generative AI and a monthly legal cybersecurity newsletter.

Looking Ahead
COVA CCI is poised for continued impact and growth. With an expanding network, a maturing innovation pipeline, and demonstrated economic and educational value, COVA CCI remains a cornerstone of Coastal Virginia's cybersecurity strategy.

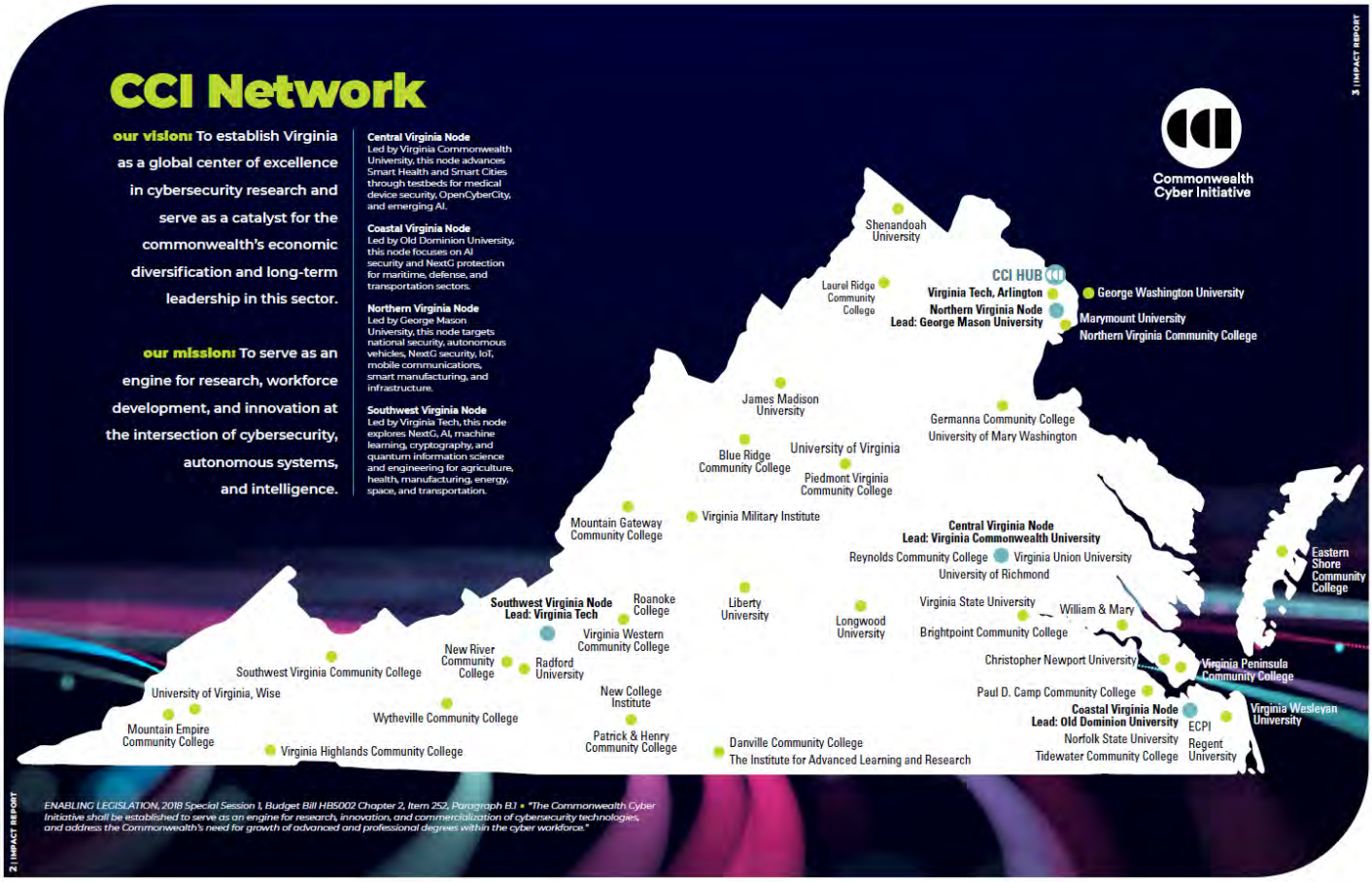
Chapter 1: COVA CCI Introduction

The Commonwealth Cyber Initiative (CCI) is Virginia's central hub for cybersecurity research, innovation, and workforce development where cutting-edge ideas take shape, talent pipelines are built, and cross-sector collaboration drives real-world impact. CCI brings together researchers, students, industry leaders, and public partners to advance cybersecurity at the intersection of autonomous systems and intelligence.

With a vision to position Virginia as a global center of excellence in cybersecurity, CCI leverages the Commonwealth's exceptional research institutions, diverse higher education system, vibrant startup ecosystem, and deep concentration of cyber talent to fuel innovation and economic growth.

Virginia's Commonwealth Cyber Initiative (CCI) aims to develop a Commonwealth-wide ecosystem of innovation in cybersecurity, with a focus on trust and security. Certified as one of the four Commonwealth Cyber Initiative (CCI) nodes, the Coastal Virginia Center for Cyber Innovation (COVA CCI) seeks to: conduct fundamental research in cybersecurity, artificial intelligence, and 5G, supporting CCI's mission to position Virginia as a global leader in secure CPS and the digital economy; promote and accelerate the commercialization of cybersecurity innovations to grow and diversify Virginia's cyber economy; expand and diversify the cybersecurity talent pipeline through investments in research and commercialization efforts; and build a collaborative network among educational institutions, businesses, and local, state, and federal agencies within the region, as well as with other CCI nodes.

COVA CCI has built a network of faculty and researchers representing the region's community colleges and universities. These educational partners include Christopher Newport University, Norfolk State University, Old Dominion University, William & Mary, Regent University, Virginia Wesleyan University, ECPI University, Eastern Shore Community College, Paul D. Camp Community College, Tidewater Community College, and Virginia Peninsula Community College. COVA CCI is also collaborating with industry and government partners such as CISCO, Deloitte, G2Ops, Huntington Ingalls Shipbuilding, KBRWyle, MITRE, MI Technical Solutions, Peregrine Technical Solutions, Sentara Healthcare, Valor Cybersecurity, U.S. Navy, and 360IT, to name a few.


CCI Network
our 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.
our mission: To serve as an engine for research, workforce development, and innovation at the intersection of cybersecurity, autonomous systems, and intelligence.
Central Virginia Node
Led by Virginia Commonwealth University, this node advances Smart Health and Smart Cities through testbeds for medical device security, OpenCyberCity, and emerging AI.
Coastal Virginia Node
Led by Old Dominion University, this node focuses on AI security and NextG protection for maritime, defense, and transportation sectors.
Northern Virginia Node
Led by George Mason University, this node targets national security, autonomous vehicles, NextG security, IoT, mobile communications, smart manufacturing, and infrastructure.
Southwest Virginia Node
Led by Virginia Tech, this node explores NextG, AI, machine learning, cryptography, and quantum information science and engineering for agriculture, health, manufacturing, energy, space, and transportation.
Commonwealth Cyber Initiative
3 | IMPACT REPORT
Shenandoah University
Laurel Ridge Community College
CCI HUB
Virginia Tech, Arlington
Northern Virginia Node
Lead: George Mason University
George Washington University
Marymount University
Northern Virginia Community College
James Madison University
Germanna Community College
University of Mary Washington
Blue Ridge Community College
University of Virginia
Piedmont Virginia Community College
Mountain Gateway Community College
Virginia Military Institute
Central Virginia Node
Lead: Virginia Commonwealth University
Reynolds Community College
Virginia Union University
University of Richmond
Eastern Shore Community College
Southwest Virginia Node
Lead: Virginia Tech
Roanoke College
Liberty University
Longwood University
Virginia State University
William & Mary
Brightpoint Community College
Virginia Western Community College
New River Community College
Radford University
Southwest Virginia Community College
Christopher Newport University
Virginia Peninsula Community College
University of Virginia, Wise
New College Institute
Paul D. Camp Community College
Coastal Virginia Node
Lead: Old Dominion University
Virginia Wesleyan University
Mountain Empire Community College
Wytheville Community College
ECPI
Patrick & Henry Community College
Norfolk State University
Regent University
Virginia Highlands Community College
Danville Community College
The Institute for Advanced Learning and Research
Tidewater Community College
2 | IMPACT REPORT
ENABLING LEGISLATION, 2018 Special Session 1, Budget Bill HB5002 Chapter 2, Item 257, Paragraph B.1 • "The Commonwealth Cyber Initiative shall be established 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."

Chapter 2: Research Programs

a. External Research Grants Attracted to Support the Work of CCI

The Commonwealth Cyber Initiative brought in $384 million in research funding over the past five years, with 30% coming from industry partners.

b. External Research Projects. During FY 2026, researchers affiliated with COVA CCI received $9,727,555 in external grant funding from various public and private organizations. Seven (7) grants came from federal agencies, and six (6) grants were from state and/or private partners.

Institution	Amount	# Grants
ODU	**$9,171,028**	**9**
WM	**$25,000**	**1**
CNU	**$76,527**	**3**
Total	**$9,272,555**	**13**

Funding Source	Amount	# Grants
Federal	**$4,900,305**	**7**
State/Private	**$4,372,250**	**6**
Total	**$9,272,555**	**13**

See the table below for the list of funded projects.

Project Name	PI/Co-PI	Lead Institution	Funding Amount	Funding Agency
Machine learning empowered O-RAN based dynamic spectrum management	Sachin Shetty, Nico Barata, Neda Moghim	ODU	$4,189,723	CACI
Enhancing Joint Live, Virtual, and Constructive (JLVC) Training Envrmt	Barry Ezell, Sachin Shetty, Ross Gore, Abhishek Phadke (CNU)	ODU	$2,319,948	Systems Engineering Research Center/DoD
SCC-IRG: Resilient Sheltering Decision Support for Emergency Evacuations using Explainable AI	Rafael Diaz	ODU	$1,250,000	NSF

Applying AI/ML to forecast community health needs and plan public/private resource allocation to mitigate the impacts of stricter FY26 Medicaid eligibility rules	Bridget Giles, Ross Gore, Neda Moghim	ODU	$612,500	HIH
Department of Defense Cyber Service Academy (DoD CSA) program at Old Dominion University	Danile Takabi	ODU	$465,027	DoW
CRII: CNS: Secure Decentralized AI in Heterogeneous IoT Networks: Foundation and Application	Qianlong "Ronnie" Wang	ODU	$145,830	NSF
IRAD Automated Threat Modeling for Agentic AI Systems	Safdar Bouk	ODU	$82,000	OERI
COVAConnectAI: Leading Coastal Virginia in AI	Rafael Diaz	ODU	$75,000	SCHEV
Empirical evaluation and open-source enablement of low-latency networking: L4S and NQB queueing architectures for improved end-user quality	Abhishek Phadke	CNU	$60,000	COMCAST
Quantitative Assessment of Hybrid Infrastructure for AI-Enabled, Multi-Disciplinary Coastal Resilience under Recurrent Tidal Flooding	Wanting (Lisa) Wang Lusi Li Sina Razzaghi Asl	ODU	$31,000	CARMA
A Knowledge-Guided Multitask LLM for Software Vulnerability Detection, Reasoning and Mitigation	Huajie (Jay) Shao	WM	$25,000	NSF
Flight Lab: Fundamentals of Drone Coding	Abhishek Phadke	CNU	$15,277	VIVA
Generating hyper-local ecosystem and terrain datasets using modified low-cost UAS platforms to support applied geospatial research	Abhishek Phadke	CNU	$1,250	Virginia Academy of Science

Research Spotlight: Enhancing Joint Live, Virtual, and Constructive (JLVC) Training Environments for Electromagnetic Spectrum (EMS) Operations and Integrated Multi-Domain Uncrewed Autonomous Systems

Barry Ezell, ODU

Ross Gore, ODU

Sachin Shetty, ODU

Yiannis Papelis, ODU

Abhishek Phadke, CNU

Old Dominion University received the award from the Stevens Institute of Technology Systems Engineering Research Center (SERC) on behalf of the Joint Staff J-7, Directorate for Joint Force Development. The project focuses on Enhancing Joint Live, Virtual, and Constructive (JLVC) Training Environments.

The effort is led by ODU's Barry Ezell, with co-principal investigators Ross Gore, Sachin Shetty, and Yiannis Papelis. The winning proposal builds on cyber-resiliency-focused generative AI work conducted by Ross Gore during the 2025 CCI Fellowship with Abhishek Phadke (Christopher Newport University).

"The support from CCI Fellowship grants allowed us to collaborate and accelerate advances in cybersecurity, AI, and resilience," Gore said. *"That foundation was instrumental in moving our work to greater technical maturity and readiness, paving the way for this award."*

The team is developing a robust framework for continuous monitoring, rapid response, and secure generative AI deployment, addressing critical defense and national security challenges at the intersection of autonomous systems and sensitive protocols. The team briefed their progress on March 18, 2026, at the project's second quarter review meeting.

This award directly builds on a foundation of CCI-funded basic research that produced three peer-reviewed publications. Gore and Ezell co-authored "AI-Generated Messaging for Life Events Using Structured Prompts: A Comparative Study of GPT With Human Experts and Machine Learning" in IEEE Access (2025), establishing a reproducible framework for validating AI-generated messaging using structured prompts and ensemble machine learning classifiers. They also contributed to "Evolving Risk Communication: Analyzing Risk Response Effectiveness of Personalized Narrative Messages," presented at the 2025 IEEE Systems and Information Engineering Design Symposium (SIEDS), which demonstrated that LLM-powered individualized narrative frameworks consistently outperform generic messaging in motivating protective action across diverse populations. Phadke, and Gore authored "Resource-Aware Adaptive Monitoring for

Smart Grid Integrity: A Comparative Analysis of Sparse and Sentinel-Augmented Sensing Modes," which developed adaptive threshold-based monitoring strategies for detecting integrity-relevant disturbances in smart power grids under constrained observability. All three publications explicitly acknowledge support from the Commonwealth Cyber Initiative (CCI), underscoring the direct line from CCI's investment in basic research to the technical readiness that enabled this award.

Visit the COVA CCI Website to learn more about their research - https://covacci.org/research/research-spotlight/

Summary of Research Grants and Programs Awarded

COVA CCI is providing research funding for several initiatives. This support has proven to be instrumental in enhancing research efforts through collaboration with fellow researchers across the CCI network.

Research Programs	Funding
FY 2026 COVA CCI Cybersecurity Research Projects	$479,926
FY 2025 COVA CCI Cybersecurity Research Projects	$406,667
FY 2026 Research Scientists Funding	$1,249,880

a. **FY 2026 COVA CCI Cybersecurity Research Program.** COVA CCI supported six research projects with $479,926 in funding in FY 2026. These projects were selected from the CCI Call for Proposals – Agentic AI Cybersecurity and Security for Agentic AI. Visit the COVA CCI Research website for more information regarding these and other funded projects - https://covacci.org/research/cybersecurity-research/.

ODU News Article: Regional Cybersecurity Hub Drives Innovation and Opportunities. "As we enter the era of the Internet of Agents (IoA), where autonomous AI agents communicate and coordinate with each other, security must be the foundational architecture, not an afterthought," Dr. Takabi said. "By funding these strategic grants, we are empowering our researchers to build the next generation of autonomous systems that act with integrity, transparency and resilience."

COVA CCI Funded Research Projects – FY 2026 – Agentic AI Security

CCI Call for Proposals	Project Title	PI	Amount
Agentic AI Cybersecurity and Security for Agentic AI Systems	Securing Agentic AI Systems using Verified Behavioral Templates	Dr. P. Giabbanelli ODU	$80,000
Agentic AI Cybersecurity and Security for Agentic AI Systems	Security and Privacy for Client-Hosted Agents via Trusted Hardware	Dr. J. Takeshita (ODU)	$80,000

Agentic AI Cybersecurity and Security for Agentic AI Systems	Agentic AI for Multi-Modal Perception Integrity: Threat Reasoning and Response in Cyber-Physical Transportation Systems	Dr. Q. Ting (ODU)	$79,926
Agentic AI Cybersecurity and Security for Agentic AI Systems	Securing Clustered Semantic Communications in Agentic AI Systems	Dr. L. Li (ODU)	$80,000
Agentic AI Cybersecurity and Security for Agentic AI Systems	Enhancing Safety of Agentic AI for High-Stakes Physical Systems	Dr. F. Liu (ODU)	$80,000
Agentic AI Cybersecurity and Security for Agentic AI Systems	Securing Mobile Agentic AI Systems: Systematic Risk Analysis and Defense Against Confused Deputy Behavior	Dr. Y. Xiao (WM)	$80,000

b. **FY 2025 COVA CCI Cybersecurity Research Program.** COVA CCI supported seven research projects with funding in FY 2025 for $406,667. These projects were selected from the CCI Call for Proposals – Cybersecurity for AI and AI in Cybersecurity. Visit the COVA CCI Research website for more information regarding these funded projects - https://covacci.org/research/cybersecurity-research/.

COVA CCI Funded Research Projects – FY 2025

CCI Call for Proposals	Project Title	PI	Amount
Cybersecurity for AI and AI for Cybersecurity	Towards a Knowledge-Guided Foundation Model for Long-Tail Anomaly Detection in Network Traffic	G. Zhou (WM)	$66,667
Cybersecurity for AI and AI for Cybersecurity	Secure and Privacy-Preserving Decentralized AI through Model Refine and Fully Homomorphic Encryption	Q. Wang (ODU)	$70,000
Cybersecurity for AI and AI for Cybersecurity	Cyber-Attack Resilient Distributed and Explainable AI with Zero Trust Architecture	R. Diaz (ODU)	$50,000
Cybersecurity for AI and AI for Cybersecurity	Toward Integrated Security and Privacy Solutions for Multi-Modal AI	L. Li (ODU)	$60,000
Cybersecurity for AI and AI for Cybersecurity	Leveraging Large Language Models for Enhanced Software Security Analysis and Malware Detection	Y. Xiong (WM)	$50,000

Cybersecurity for AI and AI for Cybersecurity	Study of Adversarial Attack Strategies on Autonomous Vehicles equipped with LiDAR Sensors	A. Phadke (CNU)	$50,000
Cybersecurity for AI and AI for Cybersecurity	Enhancing the Security of Large Language Models Against Persuasion-Based Jailbreak Attacks in Multi-Turn Dialogues.	J. Rafiei	$60,000

c. **FY 2026 CCI Funded Research Programs.** COVA CCI researchers were awarded thirteen (13) projects from CCI and three (3) from CCI NOVA during FY 2026, totaling $1,304,962.

FY 2026 CCI Research Projects	Awards	Total Funding awarded to COVA CCI
Critical Infrastructure Cybersecurity	6	$600,000
Experiential Learning Program	4	$399,962
CCI Fellows Program	1	$50,000
Cyber as a Service Program	2	$30,000
CCI Totals	**13**	**$1,079,962**
FY 2025 CCI NOVA Research Projects	**Awards**	**Total Funding awarded to COVA CCI**
2025 CATAPULT (Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology	3	$225,000
CCI NOVA Totals	3	**$225,000**
Total Funding from CCI and CCI NOVA	**16**	**$1,304,962**

FY 2026 CCI and CCI NOVA funded projects by program.

CCI Call for Proposals	Project Title	PI	Amount
Critical Infrastructure Cybersecurity	OpenCIVI:Open Benchmarks and AI-Ready Defenses for Vehicle-to-Infrastructure	Sidi Lu (WM)	$100,000
Critical Infrastructure Cybersecurity	Intelligent Framework for Securing IoT Systems in Critical Infrastructure	Mahmoud Nazzal (ODU)	$100,000
Critical Infrastructure Cybersecurity	Cyber-Resilient Multi-Sensor Radiation Monitoring for High-Energy Accelerators	Jiang Li (ODU)	$100,000

Critical Infrastructure Cybersecurity	Autonomous LLM Agents for Microgrid SOC	Mohammad GhasemiGol (ODU)	$100,000
Critical Infrastructure Cybersecurity	AI-Driven Security for Distributed Power-Grid: Integrated Layered Simulation and AI-Powered Attack/Defense Scenarios	Javad Rafiei Asl (ODU)	$100,000
Critical Infrastructure Cybersecurity	Secure LFE: Securing LF Energy's Open-Source Ecosystem for Critical Energy Infrastructure	Yue Xiao (WM)	$100,000
Experiential Learning Program	Cyber Ready: Experiential Workforce Development for Community College Learners	Chris Carter (VSGC/ODU)	$100,000
Experiential Learning Program	ACCEL: AI-native Cyber Experiential Learning for CyberWorkforce Readiness Across Hampton Roads	Safdar Bouk (ODU)	$100,000
Experiential Learning Program	Experiential Learning Program for AI-Driven Cybersecurity of RF and Edge-Enabled IoT Systems	Dimitrie Popescu (ODU)	$100,000
Experiential Learning Program	CyberBridge Fellows: A Multi-Institution Experiential Learning and Internship Program for Cybersecurity Workforce Development	Abhishek Phadke (CNU)	$99,962
CCI Fellow Program	CCI Fellow – Dr. Daniel Takabi	Daniel Takabi (ODU)	$50,000
Cyber as a Service Program	Suffolk Cyber Clinic	John Costanzo (ODU)	$15,000
Cyber as a Service Program	ODU Student led Security Operations Center	Daniel Takabi (ODU)	$15,000
FY 2026 CCI NOVA Research Projects			
CATAPULT/ASCEND Program	AETD-X: AI-Based Early Warning System for Inappropriate EMR Access	Michael Lapke (CNU)	$75,000
CATAPULT/ASCEND Program	AgentSec: Agentic AI Security Gateway	Rui Ning (ODU)	$75,000
CATAPULT/ASCEND Program	RAEMAP-Display: Decentralized Edge Processing for Privacy-First Multi-User Eye Tracking in Digital Signage	Sampath Jayarathna (ODU)	$75,000

d. **FY 2025 CCI Funded Research Programs.** COVA CCI was awarded six (6) projects from CCI and three (3) from CCI NOVA during FY 2025, totaling $739,948.

FY 2025 CCI Research Projects	Awards	Total Funding awarded to COVA CCI
CCI Cyber Clinic (WM)	1	$15,000
CCI Cyber for AI and AI for Cyber	3	$300,000
CCI Experiential Learning Program	2	$199,948
CCI Totals	**6**	**$514,948**
FY 2025 CCI NOVA Research Projects	**Awards**	**Total Funding awarded to COVA CCI**
2025 CATAPULT (Cyber Acceleration, Translation, and Advanced Prototyping for University Linked Technology	3	$225,000
CCI NOVA Totals	3	**$225,000**
Total Funding from CCI and CCI NOVA	**9**	**$739,948**

e. **Research Faculty.** COVA CCI continues to support research scientists at William & Mary and Old Dominion University (School of Cybersecurity and Virginia Modeling, Analysis, and Simulation Center), as well as an ITS engineer from ODU. Biographies for these research scientists are available on the [COVA CCI website under People, Research Scientists](#).

During FY 2026, COVA CCI supported nine (9) research scientists and one ITS Engineer.

The supported research scientists and the ITS Engineer are.

- Christina Galvagna, William & Mary
- Daniel Shin, William & Mary
- Mohammad GhasemiGol, ODU School of Cybersecurity
- Javad Asl, ODU School of Cybersecurity
- Nazmul Sikder, ODU School of Cybersecurity
- Neda Moghim, ODU VMASC
- Nico Barat, ODU VMASC
- Sandip Roy, ODU VMASC
- Soumya Banerjee, ODU VMASC
- Yogesh Sur, ODU. ITS engineer to support COVA SHARE.

f. **CCI Supply Chain Cybersecurity Cluster.** In addition to these research scientists, COVA CCI provided funding for three professors/research professors as part of a cluster hire with George Mason. The ODU cluster will focus on supply chain and maritime cybersecurity and will work with GMU faculty to pursue large government projects related to these research areas.

- Rafael Diaz, ODU, Director Supply Chain Cybersecurity Research
- Yexhou Li, ODU Research Assistant Professor
- Wael Khallouli, ODU Research Assistant Professor

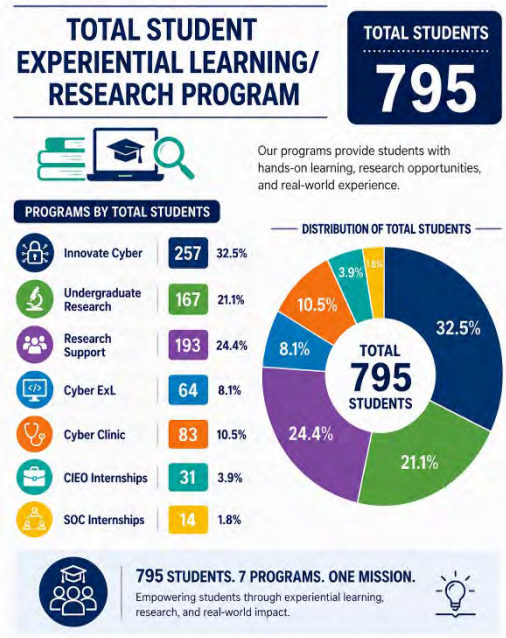
g. **COVA Shared Research Environment (COVA SHARE)**

COVA CCI continues to invest in our shared collaborative research computing environment, known as COVA SHARE, to support the growing cybersecurity programs, academic and research collaboration opportunities, and industry partnerships.

Visit the COVA CCI/Research/COVA SHARE website for additional information on COVA SHARE and watch a short overview YouTube video – What is COVA Share? – to learn more about this resource.

Chapter 3: Workforce Development and Experiential Learning Programs

COVA CCI supports several programs in innovation, workforce development, and student experiential learning. These include the Innovate Cyber Challenge, Internships, the Cybersecurity Clinic, Student Led Security Operations Center, Undergraduate Research, and student research project support. To date, COVA CCI has supported 795 students from 17 different colleges and universities in these various programs.



a. **Cybersecurity Undergraduate Research Program**.

COVA CCI supported the Cybersecurity Undergraduate Research Program in Fall 2025 and Spring 2026. A total of 31 students from Camp Community College, Christopher Newport University, Norfolk State University, Old Dominion University, Tidewater Community College, Virginia Peninsula Community College, and William & Mary completed the program during the year. This program leverages the strength of research-intensive institutions to support active research participation by undergraduate students around cybersecurity. The students' research can be found on the COVA CCI/Innovation/Undergraduate Research website.

The students' papers are uploaded into the ODU Digital Library, which allows them to be viewed and cited. As of July 8, 2026, these papers were viewed over 111,016 from 205 countries.

Source: [ODU Digital Commons, Cybersecurity Undergraduate Research, Dashboard](#).

Student Spotlight: Edward Griggs, Christopher Newport University, Cybersecurity, Undergraduate Cybersecurity Research Program

Edward Griggs participated in the Spring 2026 cohort of the Undergraduate Cybersecurity Research Program, where he wrote his paper, **Hijacking the Prompt: A Survey of Prompt Injection Attacks, Detection, and Defense in Large Language Models**.

Edward said, *"The Undergraduate Cybersecurity Research Program gave me something I couldn't have gotten anywhere else as a student, a real seat at the table on applied security work, with mentorship from people who do this for a living. It pushed me past the "study for the cert" mindset and into thinking like a researcher: forming a hypothesis, defending it, and presenting findings to people who would push back. That experience is a big part of why I'm now confident pursuing roles in SOC and detection engineering, and why I treat learning as an ongoing practice rather than a checkbox."*

b. **Innovate Cyber Challenge.**

COVA CCI completed another cohort of its Innovate Cyber Challenge in spring 2026 with a total of 41 students from eleven (11) universities & colleges. These included Christopher Newport University, George Mason University, J. Sargent Reynolds Community College, Northern Virginia Community College, Old Dominion University, Tidewater Community College, Virginia Peninsula Community College, University of Mary Washington, University of Virginia, Virginia Tech, and William &

Mary.

This program groups students into teams, and each team is assigned a cybersecurity problem/challenge. Over the semester, the teams use design thinking to produce unique solutions for the problem and present their final product during a Showcase event in April 2026. This year's challenge asked - How might we design humane, transparent, and trustworthy cybersecurity experiences that empower everyday people to understand, control, and ethically participate in the protection of their digital lives?

The teams participating in this year's cohort are.
Cyber Bridge VR
Click Smart
Trace
UpdateRadar
Breachwatch
ClearAgree
Vigil
ClearShield
SafeEarn
Vault 07

Visit the COVA CCI/Innovation/Innovate Cyber Challenge webpage to view these and previous years' projects.

Student Spotlight: Edward Griggs, Christopher Newport University, Innovate Cyber designer

As part of the COVA CCI INNOVATE Cyber Challenge, ten teams participated in a semester-long design thinking course with a focus on Cybersecurity entrepreneurial problem solving. This diverse collaboration across Virginia universities allowed students to approach the problem from multiple perspectives. Edward Griggs was one of these students, and he provided his thoughts about participating in this program.

Edward said, *"The Innovate Cyber Program was where I learned how to turn an idea into a shipped product. Our cohort built Vault 7, an interactive cybersecurity game that teaches people to recognize phishing, social engineering, and ransomware through gameplay rather than the usual thirty-minute compliance video. I came in with a sysadmin background and left understanding product design, user testing, and how to communicate technical risk to non-technical audiences. It also reinforced something I now carry into every project: the best security tools meet people where they are. Both programs together gave me technical depth and the practical, collaborative skills to actually use it, and I'm grateful to have been part of*

them."

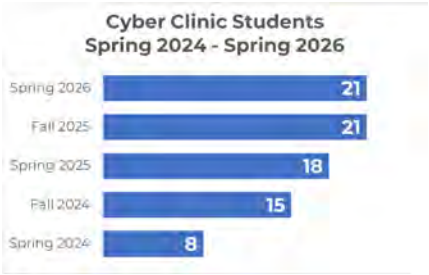
c. **COVA CCI Internships**

Cybersecurity Workforce Development – Internships. One goal of CCI and COVA CCI is to grow the cybersecurity workforce in the Commonwealth. COVA CCI is working with university researchers and business partners to achieve this goal.

Old Dominion University, with support from COVA CCI, analyzed the School of Cybersecurity internship program. The School of Cybersecurity requires its Bachelor of Science students to complete an internship as part of the cybersecurity curriculum. This is accomplished by completing CYSE 368, Internship Course. After gathering and analyzing the data for the students who completed CYSE 368 since 2019, it was determined that 909 students completed an internship experience.

Internships with CEIO. COVA CCI supported thirteen (13) interns for ODU's Center for Educational Innovation & Opportunity (CEIO). These students assisted CEIO by engaging with the diverse programming offered at CEIO and in executing hands-on STEM activities, such as field trips, family/community events, and outreach initiatives, by preparing materials, setting up equipment, and facilitating activities. Beyond event support, the interns contributed to the CEIO organizational tasks, including maintaining equipment, supporting program planning, and creating marketing materials. Their involvement extended to collaborating with community partners and providing valuable administrative assistance, allowing the iLab to offer a wide range of enriching experiences for both youth and educators. Through their work, the interns gain practical experience in program delivery, technical skills, and project management, while making significant contributions to the iLab's success.

d. **COVA CCI Cybersecurity Clinic**



Starting with a pilot cohort in the Spring 2024 semester, COVA CCI supported a Cybersecurity Clinic with eight (8) students from Old Dominion University, and two micro-businesses – a non-profit religious ministry and a government contractor. We partnered with Valor Cybersecurity, a local cybersecurity business, which provided training and subject-matter expertise to the students as they prepared to assess the client businesses. This program has continued to expand each semester. Since inception the cyber clinic supported 83 students and 25 local businesses.

This clinic offers free cybersecurity-as-a-service to small businesses, non-profits, local government offices, agencies and boards as well as other organizations. Selected students to evaluate these organization's cybersecurity readiness and risk posture. The goal of this clinic is to raise cybersecurity awareness and to provide services such as services education and risk management strategies to client organizations within Hampton Roads. It also offers students an experiential learning opportunity as cybersecurity interns/consultants. Specifically, this clinic targets those client organizations that lack a strong cyber presence and who can benefit from gaining cybersecurity knowledge through cybersecurity awareness initiatives and services.

This is a 16-week program offered during the fall and spring academic semesters. During the program, students receive training on various cybersecurity modules, enabling them to interview client organizations beginning in the middle portion of the program. The students work in teams under the guidance of ODU faculty. The team provides service to the client in one or more areas of cybersecurity, including network defense, policies and procedures, cybersecurity training for employees, cyber risk assessments, and/or cybersecurity best practices.

As of April 2025, ODU is a member of the Consortium of Cyber Clinics. The Consortium of Cybersecurity Clinics is an international network of university-based cybersecurity clinics and allies working to advance cybersecurity education for the public good.

Business Testimonial. **Blue Water Advisors**
Blue Water's cyber security posture is much improved in comparison to pre clinic attendance! We are much more proactive through education awareness of potential phishing / Spoofing attacks that pose real threats to the company. The team helped increase our awareness of cyber threats and provided valuate guidance that improved our cybersecurity posture and incident response planning. Very helpful. We are building a plan now based on the team's input!

Student testimonial regarding their experience with the Cybersecurity Clinic.

Student Spotlight, Tyler Royster, Old Dominion University, Cybersecurity, Cybersecurity Clinic Intern – Spring 2026

"One of the biggest lessons I learned is that cybersecurity is not only about technology, but also about people, planning, and effective communication."

"Throughout this experience, I worked with a team to conduct a cybersecurity risk assessment for our client business using the NIST Cybersecurity Framework (CSF) 2.0. We evaluated areas such as governance, risk management, incident response, access control, and overall cybersecurity preparedness while developing recommendations to help strengthen

the organization's security posture."

"This internship gave me valuable hands-on experience applying cybersecurity concepts in a real-world environment while also improving my communication, teamwork, and problem-solving skills.

e. Student Security Operations Center (SOC).

ODU Cybersecurity students supporting the SOC.

With support from the COVA CCI, the Student SOC provided students with the opportunity to contribute directly to ODU cybersecurity operations, while gaining practical, hands-on experience in a real SOC environment. The students worked alongside UISO security staff to support daily SOC functions, assist with Tier 1 alert response, and help expand the university's monitoring and response capacity.

The SOC serves as the central point for reviewing, triaging, escalating, and responding to cybersecurity alerts across ODU's technological environment. Its purpose is to help identify potential security incidents early, reduce institutional risk, and ensure security events are reviewed and handled consistently.

Over the course of the internship period, student interns provided Tier 1 SOC support during scheduled Student SOC coverage days. Their work included reviewing and triaging security alerts, documenting initial findings, escalating events that required further investigation, and assisting with operational requests. Students also supported firewall policy change processing, giving them exposure to both alert

response and security operations workflows.

The students reviewed more than 1,000 security alerts and supported approximately 150 firewall change requests during the reporting period. This work provided measurable operational value to the SOC by increasing Tier 1 review capacity and helping reduce the workload placed on full-time analysts. With students handling review and routine support tasks, professional SOC staff were able to spend more time on higher priority investigations, complex incidents, and process improvement.

The program also served an important workforce development role. Students gained practical experience using security tools, following documented procedures, communicating findings, and understanding how alerts move from initial review through escalation and response. This helped prepare students for cybersecurity roles while also demonstrating that a structured Student SOC model can provide real operational benefit to the university.

Overall, COVA CCI funding helped support a student-centered SOC model that strengthened security operations, expanded monitoring and response capacity, and provided students with valuable applied cybersecurity experience.

Old Dominion University wrote an article about this innovative program - Building Skills and Confidence Through a New, On-campus Cybersecurity Hands-On Learning Opportunity.

> **"We're in a position where we can provide this opportunity and help these students acquire real-world skills,"** Luke Watson, ODU deputy chief information security officer said. **"They can leave Old Dominion University having real IT security knowledge, which many don't get until three or five years into their careers."**

f. Workforce Development Programs (By the numbers)

Student Workforce Development. Since its founding in 2020, COVA CCI has supported **795** students through various programs. These students worked as research assistants on research projects and participated in the undergraduate research and Innovate Cyber programs. All students gained valuable workforce skills that they will carry into their future careers.

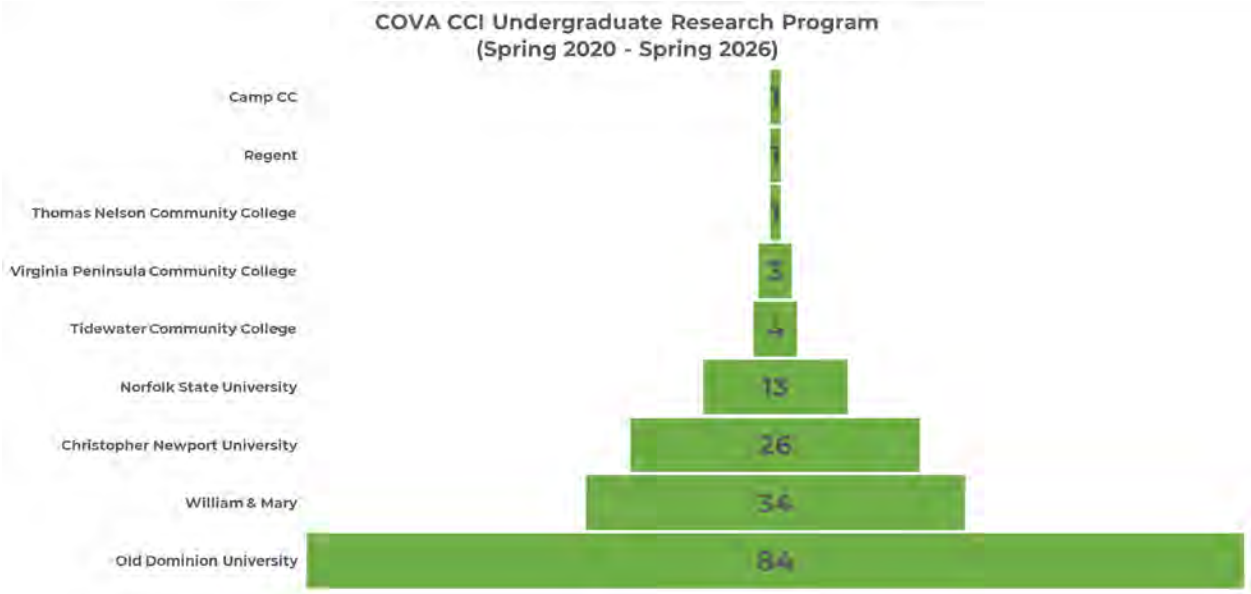
During FY 2025, a total of **141** students participated in COVA CCI Programs in Fall 2025 and Spring 2026, including Undergraduate Cybersecurity Research, Innovate Cyber Challenge, CIEO Internships, Student Led Security Operations Center, and the Cybersecurity Clinic.

COVA CCI Workforce Development Programs for Fall 2025 and Spring 2026

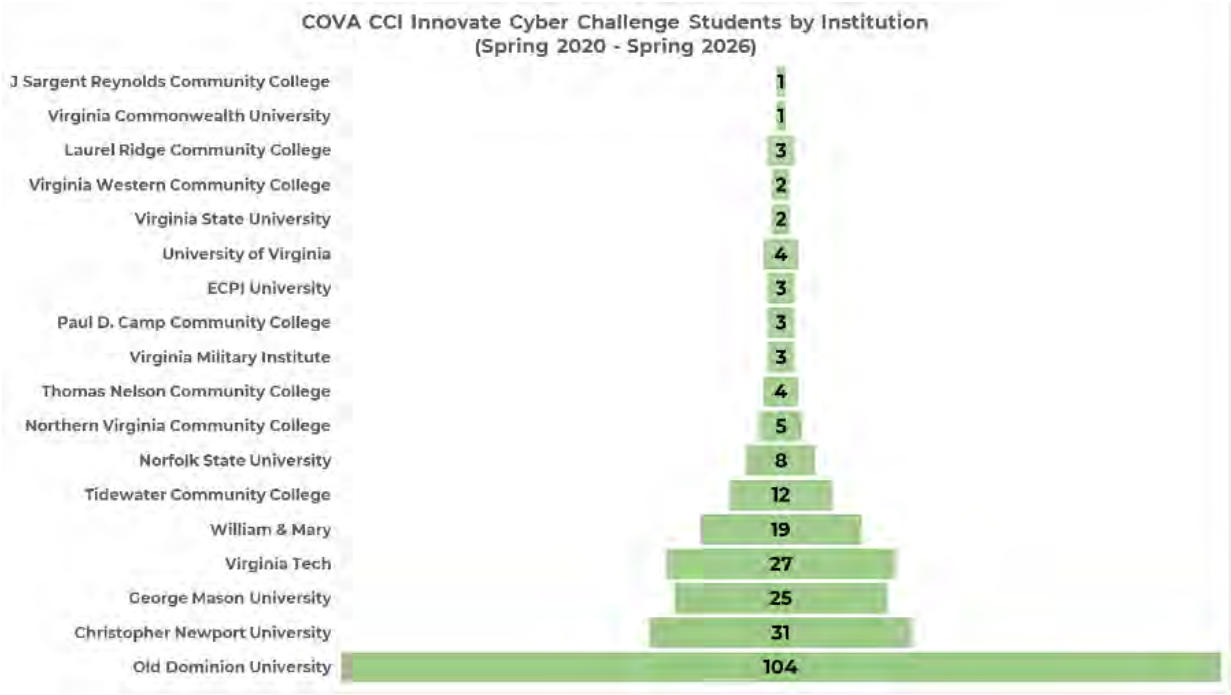
School	Total by Institution	UG Research	Innovate Cyber	CIEO Interns	Student SOC	Cyber Clinic

CNU	9	7	2			
Camp CC						
GMU	1		1			
J Sergent Reynolds CC	1		1			
NSU						
Mary Washington	3		3			
NOVA CC	1		1			
ODU	92	13	10	13	14	42
Tidewater CC	4	1	3			
Virginia Peninsula CC	4	2	2			
VT	9		9			
UVA	1		1			
W&M	16	8	8			
Total	141	31	41	18	14	33

Undergraduate Research Program – A total of **167** students from seven institutions have participated in this program since Spring 2020, with 31 students completing the program during Fall 2025 and Spring 2026 semesters.



Innovate Cyber Program – A total of **226** students from 17 institutions have participated in this program since Spring 2020, with 41 students completing the program during the Spring 2025 semester.



Cybersecurity Clinic – A total of **83** students completed the Cybersecurity Clinic since the Spring 2024 semester, with 42 completing the program in fall 2025 and spring 2026.

School	Total per Institution	Spring 2026	Fall 2025	Spring 2025	Fall 2024	Spring 2024
ODU	83	21	21	18	15	8
Total	**83**	**21**	**21**	**18**	**15**	**8**

Student led Security Operations Center – A total of **14** students completed the Cybersecurity Clinic since the Fall 2025 semester, with 14 completing the program in fall 2025 and spring 2026.

School	Total per Institution	Spring 2026	Fall 2025
ODU	14	7	**7**
Total	**14**	**7**	**7**

Research Assistants – **193** students from multiple institutions at the post-doctoral, Graduate, and Undergraduate levels. These students are supporting CCI/COVA CCI research projects/activities across multiple semesters/years.

Number of research assistants from January 2021 through June 2026	
Category	Total per Education Level

PhD	40
GRA	103
UG	50
Total	**193**

Chapter 4: Economic Impact/Innovation

a. NOVA CCI Ascend/Catapult Program. The Northern Virginia node of CCI (NOVA CCI) releases an annual call for proposals under their Commonwealth Cyber Incubator and Accelerator (CCI+A) program. This program is designed to provide researchers with the tools, mentorship, and funding needed to move discoveries beyond proof-of-concept and into viable market opportunities, and to provide companies with access to cutting-edge university research and resources to create market opportunities that benefit the commonwealth. In FY 2026, COVA CCI researchers were awarded three projects under this program.

AETD-X: AI-Based Early Warning System for Inappropriate EMR Access

Lead University: Christopher Newport University. PI-Michael Lapke
Partners: Old Dominion University, William & Mary, Neptune Shield

Abstract: Healthcare organizations operate some of the most sensitive data infrastructures in the United States. While perimeter cybersecurity has improved, Electronic Medical Record (EMR) systems remain vulnerable to inappropriate or contextually inconsistent data access. These incidents may stem from workflow deviations, policy misunderstandings, compromised credentials, or subtle misuse of legitimate privileges. Existing controls rely heavily on static role-based access control (RBAC) and retrospective audit review, both of which lack contextual awareness and impose a significant compliance burden. This project seeks CATAPULT support to commercialize **AETD-X**, an AI-driven early warning platform for real-time detection of inappropriate or anomalous access to critical healthcare data. The underlying intellectual property builds on prior CCI-supported research and models EMR access as a structured, context-rich behavioral sequence rather than as isolated audit events.

AgentSec: Agentic AI Security Gateway

Lead University: Old Dominion University. PI-Rui Ning
Partners: AgentSec LLC

AgentSec is a cybersecurity solution designed to protect agentic AI systems by delivering **one policy layer for every agent**. Acting as an agentic AI security gateway, AgentSec sits between the agent and its tools or connectors, applying deterministic, enterprise-approved policies to each planned tool invocation. Instead of building one-off guardrails per workflow, teams define policies once (for example, what tools are allowed, what data can be accessed, what requires approval, and what must be blocked) and apply them uniformly across agents, connectors, and deployments. This approach reduces operational burden, accelerates safe rollout, and produces consistent audit evidence for governance and compliance. AgentSec supports both deploy time scanning and runtime protection. At deploy time, it validates model artifacts and configurations, prompt and policy packages,

tool schemas, connector permissions, and dependencies to detect unsafe configurations and over-privileged access before release.
At runtime, it inspects plans, retrieved context provenance, and tool calls in real time, enforcing allow, block, or step-up confirmation decisions for high-impact actions. The runtime gateway produces actionable security signals and audit-ready logs that support governance practices aligned with NIST risk management guidance for AI systems.

RAEMAP-Display: Decentralized Edge Processing for Privacy-First Multi-User Eye Tracking in Digital Signage

Lead University: Old Dominion University. PI-Sampath Jayarathna

The core technical innovation of the proposed RAEMAP-Display is real-time, scalable, multiuser gaze tracking and analytics, including an edge hardware that operates directly on large-format TV displays in public and retail digital signage. Unlike existing single-user eye trackers or cloud-based webcam solutions, RAEMAP-Display enables calibration-free, privacy-preserving gaze tracking and analytics entirely at the point of engagement, such as gas stations, transit hubs, retail, and healthcare facilities. Our team's scientific discovery is that real-time, multi-user gaze estimation can be achieved with a standard off-the-shelf webcam costing less than $50, without the need for infrared illumination or specialized sensors. Traditionally, eye tracking has relied on expensive single-user infrared trackers with strict calibration protocols, making multi-user analysis impractical in natural environments. In our research, we demonstrated that a lightweight, parameter-efficient, appearance based deep learning model, combined with unsupervised domain adaptation, can achieve sub-5◦ angular accuracy in unconstrained, multi-user settings using only commodity webcams. This breakthrough establishes for the first time that accurate multi-user gaze tracking is feasible on widely available consumer hardware, significantly reducing costs and opening the door to scalable, accessible deployment.

b. Economic Impact. During 2025, CCI commissioned RTI International to conduct an economic impact assessment of the Commonwealth Cyber Initiative.

This report showed the economic impact created by CCI and its four nodes during 2024 and 2025. It was determined that COVA CCI generated $20.2 million (FY 24) and $10.3 million (FY 25) annually in labor income, which generated $1.3 million (FY 24) and $1.1 million (FY 25) in annual state and local tax revenue.

The results of the COVA CCI assessment for 2024 and 2025 are below.

Coastal Region: Economic Activity Supported by CCI Coastal in Coastal Virginia in FY 2024

	Jobs	Labor Income	Value Add	Output	State and Local Government Revenues
Direct	121	$11.9M	$14.4M	$30.3M	$0.5M
Indirect	85	$5.5M	$9.0M	$16.1M	$0.4M
Induced	68	$3.5M	$7.3M	$11.3M	$0.4M
Total	**274**	**$20.9M**	**$30.7M**	**$58.2M**	**$1.3M**

Source: CCI Impact Assessment: FY 2024-2025, RTI, September 2025

Coastal Region: Economic Activity Supported by CCI Coastal in Coastal Virginia in FY 2025

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

Source: CCI Impact Assessment: FY 2024-2025, RTI, September 2025

Chapter 5: Collaborative Partnerships and Projects

COVA CCI collaborates with academic institutions across the state on cybersecurity research projects previously mentioned in this report. Researchers are also partnering with businesses on potential federal funding opportunities and ongoing research. Some of these partners include G2Ops, MITRE, MI Technical Solutions, Port of Virginia, Valor Cybersecurity, and Peregrine Technical Solutions, among others. All projects funded through COVA CCI involve collaborations with researchers from multiple institutions and/or business partners.

During FY 2026, COVA CCI, in partnership with Old Dominion University, the City of Virginia Economic Development Office, and the Information Technology Office, held discussions about creating strategic partnerships to promote the City of Virginia and Hampton Roads to business partners. They also aimed to work with students on developing internships and potential jobs. After several meetings with key stakeholders, three working groups were established: Strategic Partnerships, Workforce Development, and IT Infrastructure. This initiative has resulted in a series of meetings with both national and international companies interested in investing and expanding their presence in the region.

Chapter 6: Financial Report

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

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

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

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

Total funding received by COVA CCI, including base budget and funding received from hub/node-supported projects.

Base Budget Allocation:	$2,500,000
Hub supported projects:	$1,079,962
Northern Node supported projects:	$225,000
Total Funding Received:	$3,239.948

Distribution of COVA CCI Allocated Funds across the node region.

Distribution of Funds Across the Node Region	
Institution	Amount
Old Dominion University *(Note 1)*	$2,145,000
William & Mary	$355,000
Total Committed Funds	**$2,500,000**
Note 1: Funding under ODU includes funds managed by the ODU Research Foundation, Virginia Space Grant Consortium (VSGC), Research Scientists Salary, and other Operations Costs	
Research Scientist Salaries	*$974,880*
Research Projects	*$399,326*
COVA CCI Staff Salaries	*$352,800*
VSGC Managed Projects Admin Support	*$5,000*
CoVA Cybersecurity Student Association	*$16,100*
UG Research (Includes payments to students from multiple institutions.)	*$36,400*
Innovate Cyber Challenge (Includes payments to students from multiple institutions.)	*$70,500*
Internships	*$17,000*
Cybersecurity Summer Camp	*$28,902*
Operations and other funds	*$244,092*
Total ODU Funds	*$2,145,000*

Chapter 7: Other COVA CCI Programs and Initiatives

a. Coastal Virginia Cybersecurity Student Association.

The Coastal Virginia Cybersecurity Student Association (CVCSA) hosted the Annual conference and Capture the Flag event, known as CyberForge, at Christopher Newport University, March 28-29, 2026. CyberForge allowed students from across Virginia to hear from cybersecurity experts, participate in a Capture-the-Flag competition, and network with fellow students.

As a part of its Coastal Connect initiative, CVCSA has unified all cyber clubs in Coastal Virginia into a regional association, significantly advancing the mission to establish a collaborative environment and facilitate resource sharing among member clubs. These clubs include Christopher Newport University, Norfolk State University, Old Dominion University, Regent University, Tidewater Community College, and William & Mary. By establishing connections with these educational institutions' cyber clubs, CVCSA aligns with CCI's objective of developing a networked approach to innovation and talent development, enabling a coordinated effort supporting tomorrow's Cybersecurity experts.

Due to the CVCSA leadership's work, they proposed and were accepted to lead an effort to expand this program across Virginia. This led to the creation of Virginia Cybersecurity Students (VCyS). Virginia Cybersecurity Students (VCyS) is a statewide association which is working on establishing 3 regional nodes like CVCSA across the commonwealth. These nodes include the Coastal Node, Central Node, Northern Node and Southwest Node. This expansion signifies CVCSA's role in scaling up local initiatives to have a statewide impact. CVCSA's various events have reached over 700 unique participants.

These student-led initiatives directly support CCI's mission by facilitating talent development, knowledge sharing, and networking, effectively bridging the gap between cyber students and industry.

To learn more about CVCSA and VCyS visit the COVA CCI Student Association Website - https://covacci.org/cvcsa/.

b. William & Mary Center for Legal & Court Technology

COVA CCI provides funding to the William & Mary Center for Legal & Court Technology to support two research professors. They focus on the legal aspects and governance of cybersecurity and artificial intelligence. Daniel Shin, JD, moderated a panel discussion in June 2026 for the General Assembly's Joint Commission on Technology and Science (JCOTS) Technology Policy Symposium.

To learn more about the William & Mary Law School, Center for Legal & Court Technology visit their website - https://www.legaltechcenter.net/

Cybersecurity Newsletter: In addition to these symposiums, William and Mary Law School, Center for Legal & Court Technology, publishes a monthly "Cybersecurity Newsletter." This newsletter written by Daniel Shin, COVA CCI Research Scientist, William & Mary contains information and analysis on multiple legal issues related to cybersecurity litigation involving cybersecurity and cyber security-related topics, cyber security regulation and policy such as the White House 2023 National Cybersecurity Strategy, data breaches, cyber security issues affecting governmental bodies, including Virginia specific matters.

To see all the Cybersecurity Newsletters visit its website - https://www.legaltechcenter.net/ai-cyber/csnewsletter/.

c. Publications.

COVA CCI-affiliated researchers and faculty continue to contribute to the cybersecurity field through various publications and conference presentations. A list of these publications can be found on the COVA CCI website - https://covacci.org/research/publications/.

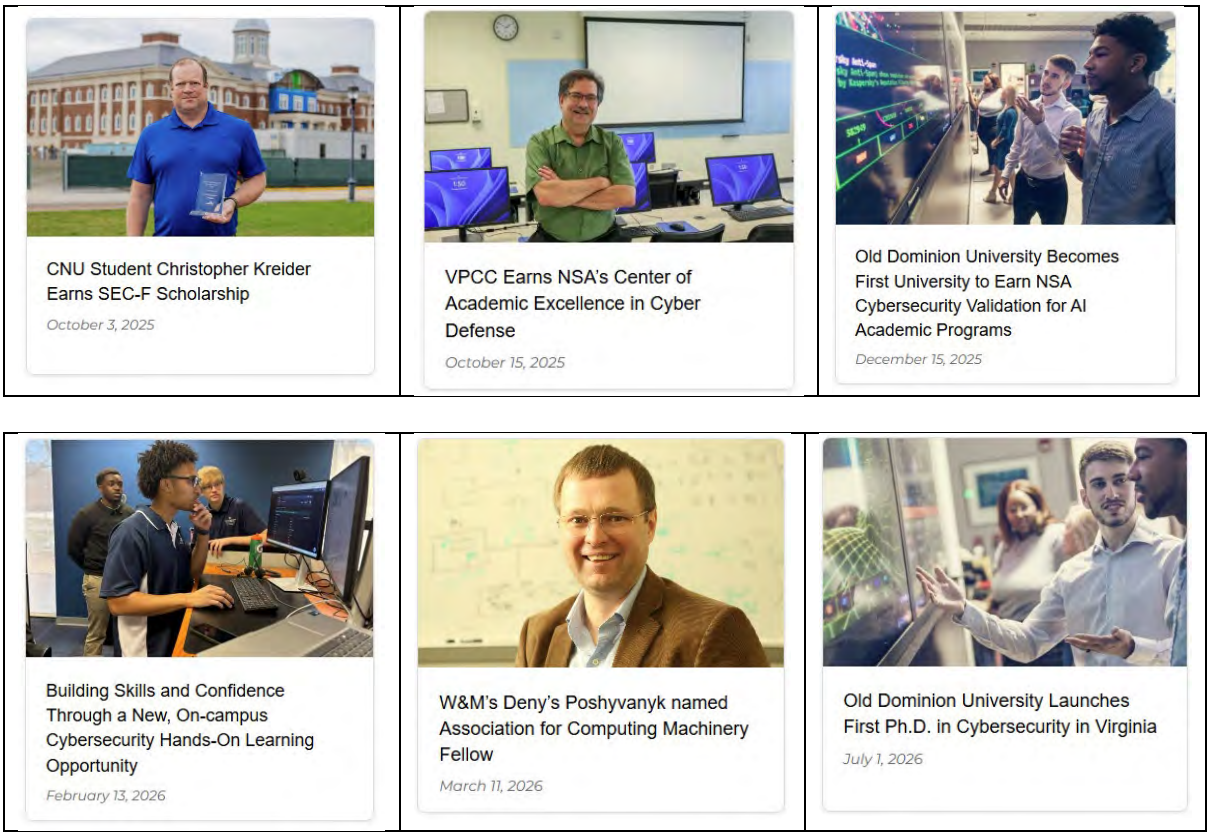
d. COVA CCI High School Cybersecurity Expo

On November 8, 2025, COVA CCI hosted a High School Cybersecurity Expo for about 70 high school students from Chesapeake Public Schools, Newport News Public Schools, Norfolk Public Schools and Virginia Beach Public Schools. During this event, the students participated in several hands-on experiences, allowing them to explore cybersecurity as a potential career field. Cybersecurity professionals from the US Navy, as well as ODU cybersecurity students, led these workshops.

e. COVA CCI Node in the News

COVA CCI has been actively promoting the success of its various activities through

local news sources. Below is a selection of some of the articles posted on the COVA CCI website – [News.]



f. Social Media via LinkedIn

We use LinkedIn to post content related to cybersecurity trends, announcements, and other activities. Over the past 365 days (July 8, 2025 – July 9, 2026, there have been 52,422 impressions on our shared posts.

g. For additional information contact John Costanzo, Chief Administrative Officer, COVA CCI, jcostanz@odu.edu, or visit the COVA CCI website (https://covacci.org) and the Commonwealth Cyber Initiative website (https://cyberinitiative.org/).

COVA CCI Website
www.covacci.org