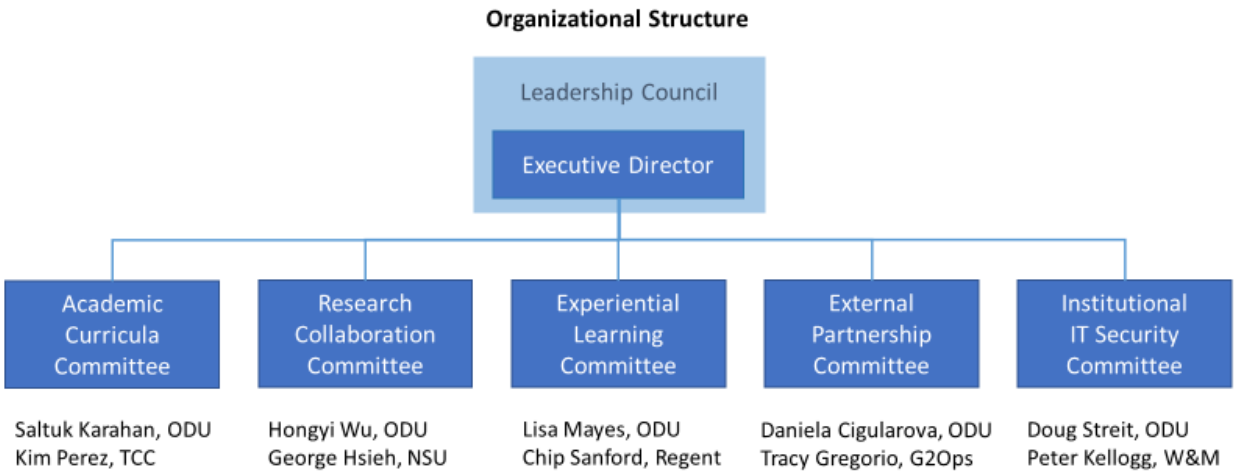
Commonwealth Cyber Initiative (CCI)
Coastal Virginia Center for Cyber Innovation
Request for Resources
FY20-FY21

Mission: The Coastal Virginia Center for Cyber Innovation (COVA CCI), as a node of the Commonwealth Cybersecurity Initiative (CCI), 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 (CPSS) and Artificial Intelligence (AI) in maritime, defense, and transportation industries. COVA CCI addresses the Commonwealth and regional needs for growth in qualified cybersecurity professionals and advanced professional degrees with the cyber workforce. The Center embraces an interdisciplinary approach taking full advantage of its member institutions' many capabilities including business, law, and marine science.

Vision: The Coastal Virginia Center for Cyber Innovation will secure the nation's critical infrastructure and strengthen Virginia's economy through the commercialization of findings from cutting-edge cybersecurity research focused on the maritime, defense, and transportation industries.



Node Executive Director: Brian K. Payne, PhD Vice Provost for Academic Affairs Professor of Sociology and Criminal Justice Old Dominion University email: bpayne@odu.edu phone: (757)683-4757	**Deputy Director:** R. Michael Robinson, PhD Director, Center for Innovative Transportation Solutions Virginia Modeling, Simulation, and Analysis Center Old Dominion University email: rmrobins@odu.edu phone: (757)638-7010
Business Partners: CISCO, Cybrex Group, G2OPs, MI Technical Solutions, Peregrine Technical Solutions, RFK Solutionz, Regent Institute for Cybersecurity, Sentara, Sera Brynn, SIMIS,SPARQ, 360IT Partners	**Higher Education Partners:** Christopher Newport University, ECPI, Eastern Shore Community College; Norfolk State University, Old Dominion University, Paul D. Camp Community College; Thomas Nelson Community College; Tidewater Community College, Thomas Nelson Community College; Virginia Cyber Alliance, Virginia Space Grant Consortium, William and Mary
Fiscal Contact: Elaine Pearson empearson@odu.edu	**Program Contact:** John P. Costanzo, MBA, PMP, LTC USA (Ret) jcostanz@odu.edu

Coastal Virginia Center for Cyber Innovation Strategic Plan

GOAL 1. BUILD WORLD-LEADING CPSS RESEARCH CAPABILITIES

The Coastal Virginia Center for Cyber Innovation will create a research ecosystem in line with the CCI vision. The COVA CCI Cyber Physical Systems Security (CPSS) research ecosystem will be built within a framework including a critical mass of nationally recognized CPSS researchers, state-of-the-art CPSS research infrastructures, and strong and vivid academic, industry, military and government partnerships. COVA CCI will support diverse and inclusive CPSS research efforts, with a focus on the intersection of artificial intelligence (AI), cybersecurity, and cyber-physical systems in the maritime, defense, and transportation sectors.

Strategy 1.A. Expand research programs applying advanced cyber technologies to the Node focus areas, to include maritime, defense, and transportation.

COVA CCI will contribute to the Commonwealth's goal of establishing a critical mass of CPSS/AI researchers. Leveraging the current cadre of cybersecurity scholars across Coastal Virginia, we will engage the following initiatives to expand the node's CPSS/AI capabilities:

Initiative 1.A.i Recruit through a regional cluster hire research faculty and research scientists to add to regional capabilities in CPSS/AI, with expertise in Artificial Intelligence and Machine Learning and next-generation wireless (5G) as related to the research focus areas of maritime, defense, and transportation industries.

These research scientists will be based in the COVA research universities (William and Mary, Norfolk State University, and Old Dominion University). They will work together under the direction of the COVA Research Committee (chaired by Hongyi Wu from ODU and George Hsieh from NSU). Pending approval of subsequent budgets, in the next biennium the research institutions will hire a cluster of eminent faculty with expertise in these areas.

Initiative 1.A.ii Develop cross-node research program to promote collaborative interdisciplinary research teams to enable holistic approaches driven by technological, social, political, legal, criminological, and ethical dimensions.

To encourage cross-institutional collaboration among current cybersecurity researchers in the node, we will provide funding and graduate research assistant support to research-qualified faculty wanting to collaborate on projects identified by the research committee and industry partners. Scholars from different disciplines and practitioners from different fields will work together to fully understand the problems and explore the design spaces. Faculty participating in the program will be expected to participate in R&D workshops, submit collaborative proposals to federal and industry agencies, contribute to ongoing projects in COVA CCI, and participate in projects across institutions in the node.

Initiative 1.A.iii Expand the pool of graduate research assistants available to help node faculty on cybersecurity research projects focused on the intersection of CPSS and AI in maritime, defense, or transportation industries.

COVA CCI will develop a pool of qualified graduate research assistants from multiple disciplines related to the node's domain areas. The graduate assistantships will be made available through the research committee to participating faculty.

Initiative 1.A.iv Create inventory of cyber faculty and cyber resources available in regional institutions.

COVA CCI will develop an inventory and portal showcasing the cybersecurity faculty participating in the node. Information to be made available in the portal will include contact information, openings, research interests, currently funded projects, research publications, patents, technical reports, opensource software, commercialization products, upcoming meetings, workshops and conferences, and other information industry partners identify as helpful. In addition, information about those resources (space and otherwise) available to be shared across the network will be identified and made available.

Strategy 1.B. Promote and support diverse and inclusive CPSS/AI research efforts, particularly in areas related to the intersection of artificial intelligence and cybersecurity in maritime, defense, and transportation industries.

Recognizing the economic opportunities in southeast Virginia, COVA CCI will incentivize and support CPSS/AI research that has the potential to produce products and start-ups of benefit to the Commonwealth. Specific initiatives will include:

Initiative 1.B.i Identify and execute collaborative research projects that leverage Node expertise.

The research committee will create research panels and bring together researchers from across the nodes to conduct fundamental research projects that have the potential to identify solutions that can be commercialized.

Initiative 1.B.ii Provide support to foster and accelerate commercialization of CPSS/AI innovation in order to grow and diversify the Virginia cyber economy.

The COVA CCI administrative office will develop tech transfer processes in consultation with the HUB. Researchers will be trained in these areas to support the commercialization efforts.

Strategy 1.C. Uplift cybersecurity research infrastructure. COVA CCI will expand shared research resources between institutions in the node, other nodes, and the Hub. Specific initiatives will include:

Initiative 1.C.i Develop secure connections and shared policies between institutional networks.

COVA CCI IT employees from across the institutions will work collaboratively to develop secure connections between institutions. The work will be led by the node's Institutional IT Security committee. A governance policy framework will be developed to guide use of the shared connections and network.

Initiative 1.C.ii Develop 5G test bed that can be used across the region and connected to the HUB 5G test bed and available to researchers from the Hub and other nodes.

Working with the Hub and other nodes, COVA CCI will create a 5G test bed to share with research institutions (William and Mary, Norfolk State University, and Old Dominion University) in the node and connect to the Hub. The test bed will be available for research, model development, simulations, and experiments by faculty and business partners affiliated with COVA CCI.

Initiative 1.C.iii Create regional testbed that uses sensors to monitor maritime transportation, including flooding resulting from climate change and sea level rise, and the impacts on transportation in flood prone areas, with capabilities to transmit data securely through a wireless network.

Drawing on regional needs in coastal Virginia, we will develop a testbed that can be used to study cybersecurity topics related to maritime transportation and flooding. The testbed will be connected across regional research institutions (William and Mary, Norfolk State University, and Old Dominion University) and will be available for research, model development, simulations, and experiments by faculty and business partners affiliated with COVA CCI.

Initiative 1.C.iv Develop the COVA Cyber Innovation Park as a location where collaborative research and experiential learning (including competitions and gaming) occurs in the Node.

The COVA CCI will be housed on the first and second floors of Monarch Hall on Old Dominion University's main campus. Roughly 11,500 square feet are planned for cybersecurity programing in that space. The space will be designated as the COVA Cyber Innovation Park. The first floor will include an experiential learning lab and faculty office space, and the second floor will include a research laboratory for COVA CCI researchers and graduate students. The COVA CCI lab will be set up so that researchers from regional research institutions will be able to connect to testbeds and other virtual programming.

Strategy 1.D. Expand connections between government, industry, and higher education to focus CPSS/AI research on topics that will help generate start-ups and products in the maritime, defense, and transportation industries.

Building on the success of the Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance (HRCYBER) and the Virginia Cyber Alliance (VCA), COVA CCI will expand its connections between regional partners. A specific focus will be given to strengthening connections that will benefit the entire cybersecurity ecosystem. Strengthening these connections, the node will engage in the following initiatives:

Initiative 1.D.i Develop inventory of business leaders and government officials who are willing and able to serve on research projects or as adjunct faculty members at one of the regional institutions.

COVA CCI will work with business partners to identify areas where they are able to share their expertise either as researchers or adjunct professors. In doing so, the business officials will gain access to those services currently available to adjuncts at the node institutions.

Initiative 1.D.ii Identify and designate space in the Cyber Innovation Park and other spaces in the node that small businesses can use for conferences and meetings.

As the Cyber Innovation Park is developed, the space will be designed in a flexible way so partnering businesses can hold planning meetings or innovation workshops in the innovation park. Additional spaces other institutions in the node are willing to share for these purposes will also be identified.

Initiative 1.D.iii Develop regional workshops focused on cybersecurity innovations.

COVA CCI will host up to three annual regional workshops designed to bring together industry and researchers so they can discuss ongoing opportunities for cyber innovation. The workshops will be held at multiple locations across the node.

Initiative 1.D.iv Build platform for cross-node research activities by implementing region-wide industry-university cooperative research center model to formalize partnerships between industry, government, and higher education.

COVA CCI will use the NSF Industry-University Cooperative Research Center (IUCRC) model to develop an industry/government research advisory board. Using a fee-based model, advisory board members will help to identify viable research projects, inventory research capabilities, foster joint SBIR/STTR proposals, provide insight into the commercialization of opportunities, develop IP sharing policies, and provide regular feedback on ongoing projects. Initially, the industry/government partners will be provided a list of possible research projects and be asked for their feedback. The research scientists and node researchers will carry out those research projects. Possible projects include:

A. Blockchain Security: With its decentralized property, blockchain is revolutionizing business operations. In particular, it has important applications in transportation and defense industry. It depends on an underlaying technology called mining. Due to their stealthy and lucrative nature, mining malwares had spiked by 629% in the first quarter of 2018 as reported by McAfee. This research will focus on the development of innovative approaches to detect malicious mining activities by using the latest CapsNet machine learning technology. [Transportation and Defense]

B. Secure Digital Manufacturing: The U.S. Navy is embracing digital manufacturing technologies to reduce maintenance costs, increase equipment readiness, and improve combat effectiveness. Digital manufacturing is heavily data driven, and thus there is an urgent need to develop efficient solutions to securing digital manufacturing data created, transmitted and processed by different entities. This research aims to employ advanced cryptography tools to develop a practical, low-cost framework to enable secure distributed digital manufacturing. [Defense Industry]

C. Secure Machine Learning: From Alexa and Google Assistant to self-driving vehicles and maritime technologies, machine learning is rapidly advancing and transforming the way we work and live. While being embraced as important tool for efficiency and productivity, it is becoming an increasingly attractive target for cybercriminals. This research will investigate new attacks to machine learning and develop a secure, accurate, and fast machine learning framework based on carefully crafted secret share techniques. [Maritime and Transportation]

D. Mobile Security: Mobile technologies are deeply integrated into defense, maritime and transportation systems. How to secure mobile devices and communication networks has become increasingly important. This research thrust will investigate a series of newfound vulnerabilities on mobile devices due to the malicious use of unsupervised sensors, and design, implement and evaluate deep learning techniques to detect and defeat attacks that exploit such vulnerabilities for information exfiltration, identify spoofing, access control, and privilege escalation. [Defense, Maritime and Transportation]

E. Secure Wireless Communication: More and more federal wireless spectrums such as the 3.5 GHz Navy radar operation band are opened by FCC and NTIA for commercial users. Spectrum authorities are turning to new technologies such as beam forming, cognitive radio and dynamic spectrum access to increase spectrum efficiency in the future 5G and 6G systems. However, wanton proliferation of these technologies and applications could open vulnerabilities and enable new forms of cyberattacks. This research aims to investigate vulnerabilities in the next generation wireless systems and develop efficient countermeasures against eavesdropping, jamming, spectrum sensing data falsification, and primary user emulation attacks. [Defense Industry]

GOAL 2. ACCELERATE CYBER STARTUP CREATION AND TECHNOLOGY COMMERCIALIZATION.

The Coastal Virginia business community has seen significant growth in the maritime, defense, and transportation sectors. With the Port of Virginia's connection to 374,000 jobs producing 17.5 billion in income across the Commonwealth and Naval Station Norfolk's identity as the world's large naval complex, the maritime, defense, and transportation industries will only continue to grow in Coastal Virginia. As these industries grow, technological changes require that new physical products and cyber initiatives have the security necessary to allow those industries to flourish. The Coastal Virginia Center for Cyber Innovation will build on its research base to promote cyber startups and technology commercialization that will support the maritime, defense, and transportation industries.

Strategy 2.A. Develop the next generation of cyber entrepreneurs, with a specific focus on promoting growth in the maritime, defense, and transportation industries.

COVA CCI will work with the HUB to create a Commonwealth-wide ecosystem of cybersecurity entrepreneurship. The node will focus specifically on start-ups and commercialization related to CPSS/AI intersections with maritime, defense, and transportation industries. Specific initiatives will include:

Initiative 2.A.i Inventory and connect with the existing innovation programs across the Coastal Virginia node.

To leverage the ability of faculty, students and businesses to create cyber start-ups and commercialize their research, COVA CCI will become a part of the regional innovation ecosystem. Specific focus will be given to working each institution's innovation office, regional innovation groups, local governments, the Open Seas Technology Innovation Hub, and Launchpad, Greater Williamsburg Business Incubator.

Initiative 2.A.ii Network and showcase innovations in annual workshops.

COVA CCI will host up to three annual workshops where faculty have the ability to present their cyber innovations to businesses and venture capitalists.

Initiative 2.A.iii Leverage the Virginia Cyber Alliance server to develop cyber experiments and simulations.

Building on the Go-Virginia Funded Virginia Cyber Alliance, COVA CCI will use the VCA lab to conduct CPSS/AI experiments related to maritime, defense, and transportation innovations.

Initiative 2.A.iv Identify entrepreneurial resources across all regional institutions and coordinate their applications.

COVA CCI will solicit information from faculty affiliates to identify institutional resources supporting entrepreneurship and innovation.

Strategy 2.B. Create processes and structure to support startups and commercialization.

In an effort to formalize the processes guiding cyber start-ups and commercialization, COVA CCI will create processes and an organizational structure that facilitates successful R&D. Coordinating with the HUB, the focus will be primarily on supporting start-ups and technology commercialization that target regional needs and opportunities for economic growth. Specific initiatives will include:

Initiative 2.B.i Develop node tech transfer processes with a specific expertise in cyber physical systems security and artificial intelligence.

Working with the HUB staff, COVA CCI will create and implement processes supporting commercialization. The processes will include mechanisms to transfer intellectual property, policies to guide the efforts, programs to increase awareness about the processes, and close collaboration with the HUB.

Initiative 2.B.ii Develop program for showcasing innovations regularly to business leaders and venture capitalists.

Working with the external partnership committee, COVA CCI will develop a formal program to connect business leaders and venture capitalists with cyber innovations occurring in the Hub. The events will include both virtual and in-person presentations as well as technical reports and proceedings and will be held at locations across the node.

Initiative 2.B.iii Develop fund for patents and proof of concept reviews.

Funds will be designated and made available upon application for patents and proof of concept review. The external partnership committee will coordinate the distribution of the funds with final recommendations made by the leadership council and subject to the approval of the node director.

Strategy 2.C. Enhance preparation of faculty and students in commercialization efforts

Commercialization strategies and technological changes have outpaced traditional strategies in the area of faculty development. For faculty to effectively commercialize their cyber work and help develop start-ups, it is important that they have training specifically targeting the tech transfer and start-up processes.

Initiative 2.C.i Develop a research leave and faculty development program allowing faculty to work in cybersecurity industry on projects leading to commercialization of intellectual property/products.

A program will be developed to better prepare cyber faculty for industry and commercialization. Components of the program will include research leave for faculty seeking to work in industry and gain industry/commercialization experience. In addition, programming (e.g., workshops) will be held better prepare cyber faculty in the areas of start-ups and commercialization.

Initiative 2.C.ii Develop a workshop training graduate students (as future faculty and entrepreneurs) about commercialization.

COVA CCI will create and implement a regional workshop training cyber graduate students about commercialization and innovation. The workshop will provide students the background they need to apply R&D topics to their future cyber research and commercialization. To provide access to all students, the workshop will be provided at locations across the node.

GOAL 3. GROW WORKFORCE-READY CYBERSECURITY AND CYBER PHYSICAL SYSTEM SECURITY TALENT TO MEET TODAY'S DEMANDS AND TOMORROW'S ECONOMY.

Institutions in the Coastal Virginia node have an established tradition of working together to respond to industry demand in the area of cybersecurity. The activities of HRCYBER and the VCA create a foundation from which we can scale our efforts to produce a current and future workforce prepared for cybersecurity careers.

Strategy 3.A. Provide more experiential learning opportunities to students.

Both HRCYBER and the VCA provided experiential learning opportunities to regional cybersecurity students. COVA CCI will build on those experiences and expand the number of cybersecurity interns and the businesses hiring those interns. The experiential learning committee will coordinate the experiential learning activities across the node. Specific initiatives will include:

Initiative 3.A.i Work with Virginia Space Grant Consortium to place additional cyber interns.

Having partnership with VSGC in the past on similar projects, the regional institutions are in a good position to leverage the momentum we have in placing cybersecurity interns in our region. Businesses will be asked to pay for 50-75% of the intern's cost, with the additional cost covered by COVA-CCI.

Initiative 3.A.ii Provide opportunities for students to engage in zero-credit internship programs.

COVA CCI will develop mechanisms so cyber students can engage in either credit-bearing or zero-credit. The zero-credit option gives students the ability to have the internship noted on their official transcripts without having to pay for the academic credit. For many cybersecurity students who have few elective options in their course plan, such an option opens the door to additional experiential learning opportunities.

Initiative 3.A.iii Strengthen business relationships to increase the number of possible internship placements.

COVA CCI will strengthen relationships we have with businesses hosting our interns. In addition to enhancing our evaluation of cybersecurity interns, business partners will be invited to participate in various activities (e.g., workshops and showcase events) held at institutions across the node.

Initiative 3.A.iv Create experiential learning opportunities for graduate students by connecting them to institutions without graduate programs.

COVA CCI will also connect our cybersecurity graduate students with students enrolled in community colleges or four-year institutions without graduate programs. Graduate students will be made available to serve as mentors or instructors in those institutions seeking graduate student support.

Strategy 3.B. Expand undergraduate research opportunities in cybersecurity for students across the node.

Each institution in the node has its own undergraduate research program. To build on existing programs, COVA CCI will create a region-wide undergraduate research program for cybersecurity students. Students selected for the program will be supervised by one of the node faculty. Specific initiatives will include:

Initiative 3.B.i Develop regional request for proposals encouraging undergraduate students and cyber node faculty to submit research proposals.

Using a common model found across regional institutions, COVA CCI will invite research proposals from cyber students enrolled in institutions in the node. The experiential learning committee will review the proposals and make funding recommendations.

Initiative 3.B.ii Host regional undergraduate research showcase.

At the end of the research project, participating students will participate in the node's annual conference. They will be required to develop and present a poster summarizing their research. Students will also be asked to identify opportunities for business start-ups or commercialization that stem from their research findings.

Strategy 3.C. Increase the number of career-ready students graduating with cybersecurity-related degrees across the node.

According to Cyberseek.org, Coastal Virginia region has the second highest number of cybersecurity job vacancies in the Commonwealth. To fill this demand, it is not enough to simply

graduate more students. Instead, institutions must increase the number of graduates, widen the diversity of cybersecurity graduates, and engage in initiatives to make sure that students are career ready. Specific initiatives will include:

Initiative 3.C.i Provide funding to K-12 instructors and faculty to support their efforts in developing programming for the Virginia Cyber Range.

Building on the success of the Virginia Cyber Range, COVA CCI will host sessions and support teachers and faculty in their efforts to make full use of the resources available through the Range.

Initiative 3.C.ii Enhance articulation agreements and transfer pathways to include apprenticeship experience, review apprenticeship training and competencies and align with higher education curriculum.

Faculty, staff, and industry partners will review the existing transfer agreements and make recommendations for changes. Specific attention will be given to expanding apprenticeships in institutions across the node.

Initiative 3.C.iii Expand opportunities for students to receive academic credit for workforce training and certifications.

COVA CCI faculty and staff will review existing policies for awarding prior learning credit. Ways to make the award of credit seamless and in line with industry standards will be suggested.

Initiative 3.C.iv Develop mechanisms to help students obtain appropriate security clearances before they enter the workforce.

Partners will work together to develop processes for getting students in the node necessary clearances as soon as possible.

Strategy 3.D. Expand entrepreneurial focus of cybersecurity students.

Preparing the future cybersecurity workforce within an entrepreneurial workforce requires that today's student be prepared for tomorrow's economy. Given the rapid technological changes and increased international focus on innovation, today's students, cybersecurity students in particular, must be prepared as innovators. To expand cybersecurity student's strengths in these areas, the following initiatives will be implemented:

Initiative 3.D.i Build business challenge.

Using the "prize challenge" as a model, COVA CCI will host a challenge incentivizing students in the node to develop a business, product, or initiative related to cybersecurity. Coordinated through the experiential learning committee, industry partners will serve as the judges in the challenge. Students will receive a cash prize.

Initiative 3.D.ii Make an entrepreneurship course available to all students in the node.

Using the resources of the Tidewater Higher Education Consortium, a course titled "Entrepreneurship for Cybersecurity" will be made available to all students in the node each summer. The course focuses on using innovation principles to develop cybersecurity businesses, products, or initiatives.

Initiative 3.D.iii Create a Cybersecurity Innovation certificate program using courses from across the region.

Partnering institutions will develop a for-credit consortium-based certificate in Cybersecurity Innovation. The online certificate program will include graduate courses from across the region, including those offered at Christopher Newport University, ECPI, Norfolk State University, Old Dominion University, and William and Mary. As part of the certificate, students will take a class where they develop a cybersecurity business or product.

GOAL 4. BUILD A COLLABORATIVE NETWORK.

The Coastal Virginia Center for Cyber Innovation with work with the other nodes and the Hub to create a collaborative network. These efforts will include routine meetings and discussions in the node, participation in Commonwealth-wide activities, collaborative programming, and consortium-based academic coursework and certificate programming.

Strategy 4.A. Develop collaborative relationships across the Coastal Virginia Center for Cyber Innovation network.

Using the CCI Blueprint as a guide, participants in the node will reach across the network to participate in activities extending across the network. In doing so, it is expected that the sum of our efforts will be greater than any individual efforts. Specific initiatives will include the following:

Initiative 4.A.i Provide a forum for collaboration among academic institutions and industry partners to align IT resources and opportunities with COVA CCI strategy and priorities.

The Institutional IT Cybersecurity Committee will work across the nodes to help align institutional needs with Commonwealth priorities.

Initiative 4.A.ii Facilitate dialogue among CIOs and technology SMEs at partner academic institutions to develop the information technology strategy to support the COVA CCI strategy.

COVA CCI will also provide CIOs from participating institutions the opportunity to develop institutional programming and policies that align with the broader Commonwealth Cyber Initiative.

Strategy 4.B. Promote collaboration between cybersecurity students

Building the collaborative network will include a focus on developing a network between cyber students in the Commonwealth of Virginia. The specific initiatives will include the following:

Initiative 4.B.i Create COVA Cybersecurity Regional Student Association.

COVA CCI will support the development of the Coastal Virginia Cybersecurity Regional Student Association. Students from each institution in the node will be invited to join. Activities will include seminars, capture the flag events, training workshops for cybersecurity-related certificates, and mentoring initiatives. These events will be held at institutions across the node.

Initiative 4.B.ii Help other nodes create regional cybersecurity student associations.

After creating the regional student association, COVA CCI will help the other nodes create similar student associations.

Initiative 4.B.iii Help Hub create statewide cybersecurity student association.

Joining the regional associations together, COVA CCI will work with the Hub to create a statewide cybersecurity student association. The node will work with the Virginia Cyber Range to host annual meetings of the Statewide Cybersecurity Student Association.

Initiative 4.B.iv Develop process for exposing businesses to students who are a part of the CCI Cybersecurity Student Association.

Working with all partners, COVA CCI will develop strategies to connect members of the student association with cybersecurity businesses.

Strategy 4.C. Promote cybersecurity offerings at all CCI institutions.

COVA CCI will work collaboratively to promote cybersecurity offerings across institutions. Where feasible, joint programming will be offered. Specific initiatives will include the following:

Initiative 4.C.i Work with Tidewater Higher Education Consortium to promote cross registration

All COVA CCI institutions are members of the consortium, which provides seamless transfer between institutions. The partnering institutions will identify strategies to promote cross-registration.

Initiative 4.C.ii Develop 2+2+1 programs helping community college students to earn graduate degrees.

The four-year institutions will work with the community colleges to provide seamless transfer between courses and, where possible, a pathway to a graduate degree in cybersecurity or a related field.

Initiative 4.C.iii Develop and maintain course listing of all cybersecurity courses offered in regional institutions.

COVA CCI will inventory all cybersecurity courses and programs offered in the node. This information will be made available on the node and hub's website.

Initiative 4.C.iv Continuously provide feedback to the curriculum development process within institutions.

COVA CCI will observe and evaluate the knowledge, skills and abilities required by the partners in the industry, military and government. The feedback from the partners will be utilized to develop new courses and modify the contents of the existing courses in accordance with the demands of the workplace.

Strategy 4.D. Develop collaborative research opportunities with other CCI nodes

The success of the COVA CCI lies in the success of the other nodes and the broader network. Recognizing the synergy between nodes, COVA CCI will engage in these initiatives:

Initiative 4.D.i Work with the HUB to promote the CCI Fellows program.

COVA CCI will work the with the CCI HUB to participate in the fellowship program, which is designed to bring faculty from across the nodes together at the HUB location on a regular basis.

Initiative 4.D.ii Participate in workshops held in the other nodes and the HUB.

Representatives from COVA CCI will participate in activities held in the other nodes as well as workshops, summits, or other events held at the HUB.

Initiative 4.D.iii Develop cross-nodes research projects.

The COVA CCI faculty will be encouraged to develop joint research projects and commercialization efforts by leveraging the complementary expertise of faculty and businesses at different nodes and the Hub.

Coastal Virginia Center for Cyber Innovation
Proposed Programs / Budget Narrative

Research

Collaborative Research Environment

The purpose of a shared COVA CCI collaborative research computing environment is to support growing cybersecurity programs, academic and research collaboration opportunities, and industry partnerships among Node member schools. Guided by the researchers in the Coastal Virginia Center for Cyber Innovation, the computing center and network investment will support the COVA CCI Node and enable communication to the Hub and other Nodes. The environment will lay a foundation to support 5G testbed data collection, secure storage and transfer between connected Node members and to the CCI Hub for analysis and other collaboration. It will provide access to a flexibly designed computing environment via connectivity improvements between ODU and William & Mary, and between ODU and Norfolk State University for potential collaborative efforts involving secure transfer of data between schools or secure remote access to physical or virtual hosts. Specifically, the CRE will include hardware to support completion of a second fiber connection between ODU and NSU, firewall capacity that will allow for robust and secure communication between ODU and other Node members, other CCI Nodes and the CCI Hub, and virtual and configurable computing and storage environment that can support multiple projects, virtual labs, academic or industry objectives. NSU and W&M could connect directly to the environment, and other schools or industry partners could have virtual access to resources. The environment will support ~200 virtual machines, 40TB of storage capacity, 4TB of RAM, 768 GHz of compute power and 10Gbps secure throughput capacity to researchers and students. The environment will also include virtualization software to allow for the automated provisioning of computing resources and allow CCI users from academia and the industry to complete cybersecurity academic and research work. The software capabilities include enhanced automation tools to better support the expected research, and licenses are included for 100 concurrent users of the on-demand virtual environment.

Future CCI Server Firewall Specifications	
Make / model	2 x Palo Alto 3260
Throughput (firewall only)	10 Gbps
Throughput (threat inspect.)	4.7 Gbps
Max sessions	3,000,000
Connections per second	118,000
Security rules	10,000

Future CCI Server & Storage Environment	
Physical Nodes	8
Storage	40TB
CPU	768 GHz
RAM	4TB
VMs	220

Interfaces	12 x 1G, 8 x 1/10G, 4 x 40G

The CRE will also include the addition of micro-segmentation and virtual firewall capabilities in the server and storage environment allows for the automated provisioning of project-based environments which would enable the COVA CCI to undertake projects that require complex protection of sensitive data.

Funding: Requested: 600,000; Contributed: 600,000

Research Scientists

A regional cluster hire of research scientists will be conducted to recruit research scientists specializing in domains related to the intersection of cyber physical systems security and artificial intelligence within the maritime, defense, and transportation sectors. The following parameters will guide the research scientist cluster hire:

- Candidates will be expected to have a record conducting research funded by the federal government or industry.
- Full-time participation in network to include joint research projects with CCI faculty to address the priorities of the Commonwealth Cyber Initiative will be required.
- Candidates will provide expertise in their specific disciplinary areas of strength.
- Those hired will serve as mentors to graduate research assistants working in CCI.
- They must be willing to partner with industry partners on joint projects
- The candidates must have or be eligible for U.S. security clearances
- Continued appointment will be based on success of the program and their ability to attain federal funding.
- Must have strong methodological skills or research skills in their area of expertise.
- The candidates will be expected to interact with industry partners, funding agencies, researchers from other nodes, national laboratories, and venture capitalists to identify opportunities for R&D.
- Candidates must collaborate with the Commonwealth's collection of partners to include industry, government, and academia on cybersecurity issues related to the intersection of cyber physical systems security, particularly in the maritime, defense, and transportation sectors.
- Candidates will provide subject matter expertise to industry partners seeking assistance with cybersecurity/AI topics

- The research scientists must possess the ability to work independently as well as demonstrated ability to work professionally and efficiently within the research group as a team player.
- The research scientist will take the lead on the development of research questions, data collection, data analysis, and writing and presenting research findings.
- The research scientists will conduct contract research and develop reports as needed.
- The research scientists will develop research proposals and budgets. It is expected that the research scientists will acquire funding to support the activities of the COVA CCI.
- Preference will be given to those who have worked in interdisciplinary and multi-institutional environment as well as those who have a strong funding record.

The institution hiring the research scientists must provide a 1:1 match equaling the amount received from CCI funding. It is anticipated that these research scientists will be located at William and Mary, Norfolk State University, the Virginia Modeling, Simulation, and Analysis Center, and Old Dominion University's Center for Cybersecurity Education and Research.

Funding: Requested: 450,000; Contributed: 450,000

Cross Node Research Projects (Faculty Time)

In an effort to promote research projects across the node institutions, COVA CCI will work with the node's research committee (which includes researchers and industry partners) to identify viable research projects, inventory research capabilities, foster joint SBIR/STTR proposals, get insight into the commercialization of opportunities, develop IP sharing policies, and receive regular feedback on ongoing projects. Initially, the research committee will be provided a list of possible research projects and be asked for their feedback. The research scientists and node researchers will carry out those research projects. Possible projects include:

A. **Blockchain Security**: With its decentralized property, blockchain is revolutionizing business operations. In particular, it has important applications in transportation and defense industry. It depends on an underlaying technology called mining. Due to their stealthy and lucrative nature, mining malwares had spiked by 629% in the first quarter of 2018 as reported by McAfee. This research will focus on the development of innovative approaches to detect malicious mining activities by using the latest CapsNet machine learning technology.

B. **Secure Digital Manufacturing**: The U.S. Navy is embracing digital manufacturing technologies to reduce maintenance costs, increase equipment readiness, and improve combat effectiveness. Digital manufacturing is heavily data driven, and thus there is an urgent need to develop efficient solutions to securing digital manufacturing data created, transmitted and processed by different entities. This research aims to employ advanced cryptography tools to develop a practical, low-cost framework to enable secure distributed digital manufacturing.

C. **Secure Machine Learning**: From Alexa and Google Assistant to self-driving vehicles and maritime technologies, machine learning is rapidly advancing and transforming the way we work and live. While being embraced as important tool for efficiency and productivity, it is becoming an increasingly attractive target for cybercriminals. This research will investigate new

attacks to machine learning and develop a secure, accurate, and fast machine learning framework based on carefully crafted secret share techniques. [Maritime and Transportation]

D. **Mobile Security**: Mobile technologies are deeply integrated into defense, maritime and transportation systems. How to secure mobile devices and communication networks has become increasingly important. This research thrust will investigate a series of newfound vulnerabilities on mobile devices due to the malicious use of unsupervised sensors, and design, implement and evaluate deep learning techniques to detect and defeat attacks that exploit such vulnerabilities for information exfiltration, identify spoofing, access control, and privilege escalation.

E. **Secure Wireless Communication**: More and more federal wireless spectrums such as the 3.5 GHz Navy radar operation band are opened by FCC and NTIA for commercial users. Spectrum authorities are turning to new technologies such as beam forming, cognitive radio and dynamic spectrum access to increase spectrum efficiency in the future 5G and 6G systems. However, wanton proliferation of these technologies and applications could open vulnerabilities and enable new forms of cyberattacks. This research aims to investigate vulnerabilities in the next generation wireless systems and develop efficient countermeasures against eavesdropping, jamming, spectrum sensing data falsification, and primary user emulation attacks.

Current projects that can be expanded will also be shared with the research committee. The committee will select those projects with the most potential to contribute to the overall goals of CCI. Faculty from across the node will be invited to participate in research projects selected by the research committee. All of the research projects supported by node funding will be multi-institutional and interdisciplinary. To be awarded funding from the node, the faculty member's institution must provide a 1:1 match in faculty time contributed to the project.

Funding: Requested: $350,000; Contributed: $350,000

Graduate Research Assistants

Graduate research assistants will be made available to the cross node research projects. The graduate assistants will include graduate students from William and Mary, Old Dominion University, Norfolk State University, and Christopher Newport University. Students will come from master's, doctoral, and law programs from those institutions. Students will be matched with projects their mentors are working and those that are related to their strengths and interests. The home institution of the graduate students funded by COVA CCI will contribute an equivalent amount of graduate assistant time to cybersecurity programming benefitting the node.

Funding: Requested: $125,000; Contributed: $125,000

Faculty Time for Research and Development

Programming will be made available to better prepare cybersecurity faculty with the commercialization process. Two specific strategies will be implemented. First, CoVA CCI will develop a "researcher-in-residence" program that embeds a cybersecurity researcher in an industry partner for a specified amount. Such a relationship will better prepare the researcher for industry/commercialization processes. Specific MOUs will be developed with each participating industry identifying expectations of each partner. Second, workshops will be held across the node to better prepare cyber faculty and graduate assistants as entrepreneurs and innovators.

The workshop programming will be designed to help researchers become more familiar with commercialization processes and start-ups. To be awarded funding from the node, the faculty member's institution must provide a 1:1 match in faculty time contributed to the project.

Funding: Requested: $300,000; Contributed: $300,000

REGIONAL INNOVATION AND TALENT PIPELINE

Internships

The Center for Cyber Innovation Cybersecurity Internship Program will provide internships for those seeking cybersecurity experience. This program builds on the previously successful grant-supported internship programs administered by the Hampton Roads Cybersecurity Education, Workforce, and Economic Development Alliance and the Virginia Cyber Alliance (VCA). Using a similar model to what was used in the past, the Center for Cyber Innovation will contract with the Virginia Space Grant Consortium to facilitate the administrative aspects of the program. VSGC facilitates internships for community college and university students and for qualified members of the military leaving active service on behalf of the VCA. Individuals interested in serving as interns apply via the Commonwealth STEM Industry Internship Program (CSIIP) via the CSIIP website: https://csiip.spacegrant.org/students. Interns must be US Citizens or Permanent Residents18 years old or older. Students must be undergraduates attending or recent graduates of 2-year or 4-year higher education institution with majors in a field of interest to VCA companies. Students must have a GPA of at least 2.7 on a 4.0 scale. Exiting military must have experience in cybersecurity or related fields. Companies or organizations interested in providing internships complete applications at: https://csiip.spacegrant.org/companies. Participating companies or organizations must provide internships within the VCA-served region and are reimbursed a portion of internship costs. (VCA limits current subsidies to $2200/student). There is no limit to the number of internships provided by a single host and hosts are encouraged to provide multiple internships. Internships are available year-round. VSGC works with employers to develop effective plans for internships with the goal of providing both valuable service to employers and effective learning opportunities for interns. Nineteen employers currently offer internships. VSGC ensures applicants meet minimum requirements and seeks to match those seeking internships with the skills or capabilities requested by specific employers. VSGC also provides end-of-program and end of internship evaluations and conducts longitudinal surveys on students' next steps for employment or graduate school.

As part of the internship program, participating businesses will be asked to pay for 50-75% of the intern's cost, with the additional cost covered by COVA CCI. In addition, to reduce the costs of for-credit internships, the program will an include a zero-credit option for students. Doing so reduces the educational costs incurred to students.

COVA CCI will strengthen relationships we have with businesses hosting our interns. In addition to enhancing our evaluation of cybersecurity interns, business partners will be invited to participate in various activities (e.g., workshops and showcase events) held at institutions across the node.

Funding for interns: Requested: $50,000; Contributed: $50,000

Funding for program support: Requested: $25,000; Contributed: $25,000

Undergraduate Research

To promote experiential learning and strengthen the pipeline of cybersecurity research, COVA CCI will develop and implement an undergraduate cybersecurity research program. The program will be based on undergraduate research programming currently underway in COVA

institutions. These current programs, some of which are funded by the National Science Foundation, will be extended to be multi-institutional and interdisciplinary. In addition, the COVA CCI undergraduate research program will leverage industry partnerships so that students learn about both cybersecurity research and cybersecurity commercialization. Cybersecurity students from across the regional institutions will have the opportunity to apply for cybersecurity undergraduate research projects. Students will be asked to develop an electronic portfolio showcasing their research. Participating students will be asked to present their research at COVA CCI workshops. In addition, at the conclusion of the undergraduate research project, the students will be encouraged to present their work at conferences and produce publishable research projects.

Funding: Requested: $50,000; Contributed: $50,000

Cyber Innovation Challenge

COVA CCI will develop a cyber innovation challenge encouraging student teams from the regional institutions to design a product or solution to a cyber challenge. Student teams will work under the supervision of node faculty trained in innovation and design thinking. A selection process will be used to identify participating students. Industry partners will be asked to rate the products/solutions. Students will receive various levels of funding depending on the ratings given to their products or solutions. Students will be asked to develop an electronic portfolio showcasing their designed product or business. Participating students will be asked to present their innovations at COVA CCI workshops.

Funding: Requested: $25,000; Contributed: $25,000

Curricula Development for Cyber Range and Coursework

To encourage utilization of the Cyber Range and curricula development across the node, COVA CCI will provide support to faculty members seeking to develop cybersecurity curricula. Faculty will be encouraged to identify gaps in existing curricula and propose strategies to fill those gaps. Workshops promoting the Cyber Range and curricula development will be held across the node institutions. Faculty receiving support will be expected to share their curricula with others in the Commonwealth. To be awarded funding from the node, the faculty member's institution must provide a 1:1 match in faculty time contributed to the project.

Funding: Requested: $100,000; Contributed: $100,000

Graduate Student Experiential Learning

Graduate student experiential learning programming will be developed in a way that benefits all partners participating in the node. One strategy that will be implemented entails having graduate students from the research institutions (William and Mary, Norfolk State, and Old Dominion) funded to provide services such as instruction or mentoring to those institutions seeking support that the graduate students are qualified to provide. Another strategy will entail pairing up graduate students with undergraduate students so that the more advanced students are able to oversee undergraduate cybersecurity programming. In some cases, graduate assistants may be made available to industry partners so that the student can provide necessary services that benefit the partner while providing a learning opportunity for the student. The home institution of

the graduate students funded by COVA CCI will contribute an equivalent amount of graduate assistant time to cybersecurity programming benefitting the node.

Funding: Requested: $100,000; Contributed: $100,000

Tech Transfer/Patent Costs/Proof of Concept Funds

To support innovation and commercialization processes, COVA CCI will provide funding to advance tech transfer. These funds will include support for patent costs and proof of concept funding. The chairs of the research and external partnership committees will review applications for these funds and make recommendations about their utilization to the Director and Deputy Director. The Director and Deputy Director will review the recommendations and consult the applicants where appropriate. After reviewing the application and recommendation, the Director will decide whether funds will be allocated.

Funding: Requested: $100,000; Contributed: $100,000

OPERATIONS

A project manager (1 FTE) and part-time administrative assistant will be hired to coordinate all activities in the node. Duties of the project manager include:

- Project management to include the following:
    - Serving as the primary point of contact for scheduling and coordinating node functions and meetings.
    - Coordinating logistical details of node projects.
    - Working closely with stakeholders and node partners to carry out the initiatives outlined in the strategic plan.
    - Developing presentations related to node activities for the director and PI.
    - Manage resources related to the initiatives identified in the node strategic plan.
    - Coordinating select cybersecurity research projects submitted through Center for Cybersecurity Education and Research, VMASC and cyber research centers at William and Mary and Norfolk State.
    - Assisting node committees in carrying out their functions
    - Assisting regional institutions with cybersecurity projects
    - Developing budgets
- Supervision to include the following:
    - Supervising part-time staff, graduate assistants, and student-workers in the COVA CCI.
    - Scheduling work hours for office staff, graduate assistants, and student workers.
    - Managing conflicts arising between those working in the office and those interacting with the office staff.
    - Reviewing the activities of office staff, graduate assistants, and student workers
- Representing the COVA CCI to include:
    - Serving as an ad-hoc committee member on all node committees
    - Communicating regularly with stakeholders about the activities of the COVA CCI
    - Participating in statewide meetings hosted by the Commonwealth Cyber Initiative
    - Serving as a budget delegate for the node director and deputy director
    - Grant writing and report writing
    - Developing and maintaining relationships with regional businesses
- Assessment duties to include:
    - Coordinating assessment of node projects
    - Writing reports summarizing the success of initiatives completed by node partners.
    - Identifying strategies to improve stakeholders' efforts in completing initiatives identified in strategic plan
    - Recommending changes to improve processes

In addition to the project manager, a part-time assistant will be hired to help with daily office oversight. As well, operation funds will be used to support other operation costs such as

workshops, non-personnel services, travel for events related to CCI, and other related activities.

The Node Director (Brian K. Payne) and Deputy Director (Mike Robinson) will contribute portions of their time to administering the activities of the node and participating in/supervising the research, innovation, and talent development activities described above.

Funding: Requested: 250,000; Contributed: 250,000.

SUMMARY OF FUNDS CONTRIBUTED BY NODE

		Node Contribution Summary	Amount
Operations	Administration	Payne will contribute 35% of his time and Robinson will contribute 25% of his time.	250,000
Research	Collaborative research environment created by IT from NSU, ODU, and WM with input from research committee.	IDC will be contributed to cover costs.	600,000
	Research scientists	Each institution hiring a research scientist (NSU, ODU, and WM) will provide a 1:1 salary match.	450,000
	Cross-node research program.	Each institution with a faculty member participating in the cross-node research project will provide a 1:1 match in faculty time. Robinson will contribute 10% of his time towards research.	350,000
	Graduate research assistants	Each institution receiving a graduate research assistant will contribute the equivalent amount of graduate research assistant time to cybersecurity research in the node.	300,000
	Faculty time for R&D	Each institution with a faculty member participating in the R&D programming will provide a 1:1 match in salary time.	125,000
Regional Innovation and Talent Pipeline	Internships	Businesses will provide a 1:1 match	50,000
	Undergraduate research	NSF grants and ONR grants will be used to match UGR projects and each node institution will be asked to contribute faculty time to supervise undergraduate research projects	50,000
	Cyber innovation challenge	ODU will contribute faculty time to supervise the project and activities of the Monarch Innovate Program will be contributed to the project.	25,000
	Faculty time for curricula	Each institution with a faculty member participating in the curricula development/cyber range preps will provide a 1:1 match in faculty time.	100,000

	development/cyber range preparations		
	Graduate student experiential learning	Each institution receiving a graduate research assistant will contribute the equivalent amount of graduate research assistant time to cybersecurity experiential learning in the node.	100,000
	Internship placement support	Business will provide fully funded internships totaling 25,000.	25,000
	Tech transfer office support/patent costs	IDC will be contributed to cover costs	50,000
	Proof of concept funds	IDC will be contributed to cover costs.	50,000

Other contributions: ODU is contributing up to 1.5M to build the Cyber Innovation Park. Current funded cybersecurity projects from William and Mary, Norfolk State, and ODU will also be used as node contributed funds where appropriate. A summary of these projects is available per request.

REQUEST FOR CAPITAL FUNDING

Request for Bond Funding

Pursuant to Chapter 2, 2018 Special Session 1, Item 252 B.6, the Coastal Virginia Node, through Old Dominion University, is requesting $1 million of the bond funds authorized in Item C-52.10 of Chapter 836, 2017 Session.

The Coastal Virginia Center for Innovation (COVA CCI) will be housed on the first and second floors of Monarch Hall on Old Dominion University's main campus. Roughly 11,500 square feet are planned for cybersecurity programing in that space. The first floor will include an experiential learning lab and faculty office space, and the second floor will include a research laboratory for COVA CCI researchers and graduate students. The COVA CCI lab will be set up so that researchers from regional research institutions will be able to connect to testbeds and other virtual programming.

Of the $5M in authorized capital funding for CCI, $500K is requested for current space renovation and preparation for the Coastal Node, broken down as follows:

• FY20 - $500K for facilities renovations and improvements

The lab will be equipped with equipment that provides a platform for research in cyber-physical system security, with a focus on artificial intelligence and visualization. This equipment will support both the research that is conducted at the Node, as well as that across the Network.

The total costs for the renovation (not including equipment) is estimated to be $2M. Old Dominion University will match the bond funds to complete the project.

Upon approval by VRIC of this request, Old Dominion University will collaborate with both the Department of Planning and Budget and with Treasury to confirm the utilization of the funds in a manner consistent with the Commonwealth's practices for capital projects and the utilization of bonds issued by the Commonwealth.