Commonwealth
Cyber Initiative

Northern Virginia

Strategic Plan
FY20-F21

Vision: The CCI NoVa Node is comprised of more than 75 partners representing academic institutions of higher education, industry and government entities, economic development authorities, non-profit organizations and P-12 school systems who anchor the pipeline of future cyber security professionals and autonomy, and security, promoting technology commercialization and entrepreneurship, and preparing future generations of diverse practitioners, innovators, educators, and research leaders, the NOVA-Node is poised to play an outsized role in ensuring the Commonwealth is recognized as a global leader in trustworthy CPS and in the tech innovation economy more broadly for decades to come.

Developed through a consensus building process, the NoVa Node strategic plan addresses the four goals of CCI. The Proposed NoVa Node Programs were also curated through a consensus building process and support shared equipment and resources, scalable results and knowledge, and technology transfer. From these efforts, new partnerships across institutions have been forged and all partners have been engaged in program formation, and will benefit from their output.

Our plans are ambitious and represent a long view to positioning NoVa and the larger Commonwealth as the leader in CPSS. In addition to CCI funding, we will seek external sponsors to support our plans and also work together to leverage ongoing activities where convergence of our efforts and pooling of resources will enable faster and wider scale of the goals. These efforts are ongoing and complement the resources we receive from CCI. In the request described herein, we seek seed resources to augment our own investments in these initiatives.

NoVa Node Organization

Node Executive Director:

Liza Wilson Durant, PhD

Associate Dean, Strategic Initiatives and Community Engagement and Professor
Volgenau School of Engineering
George Mason University
email: Ldurant2@gmu.edu
phone: .301.806.2393

NoVa Node Co-Chairs:
Victor Hoskins – President and CEO, Fairfax Economic Development Authority

Steven Partridge – Vice President for Workforce Development, Northern Virginia Community College

Leadership Council: Liza Wilson Durant (Mason), Steven Partridge (NOVA), Victor Hoskins (Fairfax Economic Development), Diana Burley (GWU), Diana Merkel (GCC), Sharon Simmons (JMU), Henry Coffman (LFCC), Diane Murphy (MU), Adrienne Bloss (SU), Andrew Marshall (UMW), Patrick Murphy (Arlington Public Schools), Stephanie Holt (Fairfax County Public Schools), John Wood (Telos), Kelly Shannon (Booz Allen Hamilton), Tom Curley (IOMAXIS), John Elliot (SPGlobal), Robert Lazaro (NVRC), and Eileen Ellsworth (Community Foundation for Northern Virginia).

Higher Education Partners:
Germanna Community College, George Washington University, James Madison University, Lord Fairfax Community College, Marymount University, George Mason University (lead), Northern Virginia Community College (co-lead), Shenandoah University, University of Mary Washington

Business Partners:
Amazon Web Services, Inc., ARAR Technology, Booz Allen Hamilton, CACI, CGI Federal, Crossroads Innovation Group, Cybervista, DEKRA, DISYS, Hilton, IAI and DGS, LLC, ICF, IOMAXIS, MITRE, SAIC, SparkLabs, SPGlobal, SPG Institute, Splunk Inc., SYSUSA, Techflow Inc., Telos Corp., U.Group, and Whole Point Systems.

Other Partners:
Economic Development: Arlington, Fairfax (co-lead), Loudoun, Prince William;
P-12 Schools: Alexandria City, Arlington, Culpeper Fairfax, Fauquier, Frederick, Loudoun, Prince William, Spotsylvania, Stafford, Warren, Winchester
Non-profits: Community Foundation for Northern Virginia, the Northern Virginia Regional Commission (NVRC), Northern Virginia Technology Council (NVTC), Northern Virginia Community, Military and Federal Facility Partnership, DCA Live, Arlington Community Foundation, Eastern Foundry, Rosie Riveters, Virginia Microelectronics Consortium, Women's Society of Cyberjutsu, Women in Tech, 1776, Shenandoah Valley Innovation Coalition, Shenandoah Valley Angel Investors, Children's Science Center, MACH37, Fredericksburg Regional Alliance, Arlington Partnership for Affordable Housing, Girls Inspired & Ready to Lead, Inc., Girls Computing League, Chambers of Commerce

Commonwealth Cyber Initiative (CCI) Northern Virginia Node Strategic Plan

GOAL 1: BUILD WORLD-LEADING CPSS RESEARCH CAPABILITIES

Strategy 1.A: Develop cross-node research programs to promote collaborative interdisciplinary research teams to enable applying advanced cyber technologies to Node focus areas

The strategic areas of focus are areas where our geographical location in the Northern Virginia Region, the interests and challenges of the constituents of the region, or the expertise of the university and industry researchers in the region confer some significant advantage in terms of strategic impact compared to other regions. These strategic focus areas will evolve over time as the CCI scales across the Commonwealth and new cybersecurity challenges emerge. It is expected that CCI NoVa Node partners will endeavor to collaborate on research initiatives that fall under these strategic focus areas and initiatives in order to build multi-institution capability. The testbeds and labs developed under these CCI initiatives will be shared resources serving the NoVa Node. CCI resources will be requested to support some of the initiatives under these Strategic Focus areas. The NoVa Node will actively seek other resources outside the CCI to support some of the initiatives not addressed with CCI funding and described herein.

Strategic Focus Area 1.A.i: Cyber Security of Transportation Network

Potential initiatives include the following:

Initiative 1.A.i.a: 5G and Autonomous Vehicle Communication

Given safety requirements of vehicles, the network that supports different types of vehicular communication, such as V2V (vehicle-to-vehicle) and V2N (vehicle-to-network), must be secure and reliable. The term V2X (vehicle-to-everything) denotes communication from the vehicle to any other device or entity, and the emerging "C-VTX" (Cellular-VTX) protocols described by 3GPP will need to be tested in realistic environments. Vulnerability assessments of C-V2X devices and modes of operations of the emerging 3GPP 5G C-V2X communication mode will be performed in a 5G testbed, and trade-offs for security and performance will be made from analysis of the results. C-V2X is still evolving and as a community we can contribute to the development, field validation and safety/cyber security verifications.

In addition, safety cases developed by National Highway Safety Traffic Administration (NHSTA) and Society of Automotive Engineers (SAE) need to be tested under different environments. NHSTA has also called out a

Notice of Proposed Rulemaking (NPRM) from industry to weigh in on the version of the 5G (i.e. GFDM vs. 5G NR) (https://www.regulations.gov/docket?D=DOT-OST-2018-0210). In addition, AutoTalk has created a new chipset that can process Dedicated Short Range Communications (DSRC) and 5G C-V2X packets on the same processor (https://www.auto-talks.com/technology/global_v2x_dsrc-and-c-v2x/) and presents another test opportunity.

Initiative 1.A.i.a: Resilience of Transportation Network to Cyber Effects

Despite our best efforts, it is not possible to guarantee protection against any and all cyber intrusions. Transportation systems must be designed for resilience against compromise. Some examples of design methodologies include isolation of a compromised segment of the network against infecting the rest of the network; graceful degradation of functionality when part of the network becomes compromised; and capability for human override if safety-critical functionality becomes compromised.

Strategic Focus Area 1.A.ii: Cyber Research for the National Defense

The fundamental importance of the cyber domain to the national defense is evidenced by the creation in 2009 of the United States Cyber Command as one of the unified commands of the United States Department of Defense. As the boundaries between the physical and the information domain become increasingly blurry, as our military forces and society as a whole become ever more connected, the potential for breakthrough advances is accompanied by the danger of exploitation by our adversaries. Information can be a force multiplier, allowing a smaller force to exert influence far beyond its size. On the other hand, as our forces and our society become more reliant on connectivity and information technology, a disabling attack on our information infrastructure can cripple our military and our society in unprecedented ways. Recent years have seen exploitation of our highly interconnected society by sophisticated information warfare operations. Research is needed to defend our increasingly interconnected society, and maintain our defense forces' ability to conduct operations. Potential initiatives include the following:

Initiative 1.A.ii.a: Security of 5G telecommunications, including protections against malicious intrusions and maintaining resilience in the face of compromised networks.

Initiative 1.A.ii.b: Research on effective military use of RF spectrum, including effective use of spectrum hopping capabilities, effective allocation of spectrum to support military needs, and policies for spectrum allocation.

Initiative 1.A.ii.c: Technologies and protocols for secure interoperability among US systems and between US and allied systems.

Initiative 1.A.ii.d: Research on cyber policy, including policies for secure interoperation with diverse systems and multi-level security; military doctrines for cyber operations; policies to support missions other than war and the capability to interoperate with NGOs and civilian agencies when military forces are called to support disaster relief.

Initiative 1.A.ii.e: Research on protecting populations from the effects of information operations and protecting our government's ability to function in the face of information operations.

Initiative 1.A.ii.f: Protection of US critical infrastructure against cyber attacks; approaches to improving resilience of operation of critical infrastructure in the event of compromise of part of the system.

Initiative 1.A.ii.g: Research on offensive cyber capabilities and strategies.

Initiative 1.A.ii.h: 5G capabilities for direct-connections between military satellites and field vehicle convoys and dismounted warfighters to communicate in radio-unfriendly environments.

Initiative 1.A.ii.i: Evolution of Defense Switched Network (DSN) and Defense Red Switch Network (DRSN) systems into 5G cellular networks

Strategic Focus Area 1.A.iii: Impact of Human Behavior on Cyber Security and Resilience of Cyber systems to Human Behavior

Potential initiatives include the following:

Initiative 1.A.iii.a: Impact of Human Behavior on Cyber Security

IBM’s 2014 Cyber Security Intelligence Index revealed that 95% of all security breaches are the result of human error. Examples include clicking on a bad link, opening the wrong email attachment, or using an insecure USB drive. Human error is not limited to end users. Computer engineers may develop code in ways that compromise the security of their software; IT administrators may not set up security systems properly. Challenges around understanding and addressing human behavioral factors and the impact of human behavior on cybersecurity present rich opportunities for making the human-cyber security loop in organizations more robust. In particular, the lens of behavioral science in concert with machine learning technologies can lead to better understanding of these human factor challenges. User behavior analytics promises to detect erroneous or malicious user activity that could lead to breaches. Work along this initiative presents opportunities to bring together a broad network of experts from academia to industry and leverage their knowledge and experience to identify behavioral factors that impact cybersecurity.

Initiative 1.A.iii.b: Resilience of Cyber systems to Human Behavior

A common reaction to an unanticipated cybersecurity threat is to harden the system by adding new rules and regulations. Over-regulation unintentionally increases time and effort that employees spend on training and policy implementation and may indeed result in rendering organizations more vulnerable to cyber threats. In addition, as each organization, including federal and state entities, have their own intrinsic protocols and internal dynamics of implementing new policies, organizations end up implementing varying cyber defense strategies. How resilient is a cyber system to over- versus under-regulation? In light of varying approaches across diverse organizations to the same or similar cybersecurity threats, are more resilient systems easily identifiable? Seeking answers to these questions necessitates bringing together various partners across academia, industry, and federal and state entities to converge to easy-to-implement and follow regulatory models that additionally account for cybersecurity human factors and an organization's regulatory environment.

Initiative 1.A.iii.c: Robust and Adaptive Cyber-Human Systems

The goal of better understanding the impact of human behavior on cybersecurity and the resilience of a cyber system to different regulatory models needs to ultimately lead to a robust cyber-human system for cyber security. Not all human behavior can be corrected on all employees, and no single system can be universally robust against all cyber threats. Therefore, work on building adaptive systems presents a rich line of research that brings together various areas of expertise, from behavioral research, to cyber security, and machine learning, and experts from diverse organizations, spanning academia and industry. Work on cyber-human systems goes beyond the goal of cybersecurity, covering research in human-computer interaction such as interaction of humans with AI systems more broadly. Thus presenting even further opportunities for critical research appealing to funding agencies, such as the National Science Foundation (IIS: CHS) and other entities of the federal government. Indeed, man-machine teaming is a key component of the Pentagon's so-called “third offset strategy,” which seeks to give the U.S. military a technological edge on the battlefield against sophisticated adversaries.

Strategic Focus Area 1.A.iv: Cyber Security of Electric/Power Distribution

Potential initiatives include the following:

Initiative 1.A.iv.a: 5G for Electricity Distribution /Power transfer:

Ways in which energy is generated and consumed are rapidly changing. Utilities are one of the prime targets for 5G applications as the energy sector has increasing requirements for monitoring and control driven by regulatory and commercial pressures. The big issues for utilities are cost, reliability and confidence in the supply chain. The availability and resilience of a communications system is more a feature of network design, operation and maintenance than it is of the technology employed. There is nothing inherent in 5G to make it more reliable and resilient than previous generations of technology; on the contrary, there is the potential that the extra infrastructure needed to provide 5G, located closer to the end service points, will increase the cost of enhancing reliability. Since all modern communications networks are software controlled, this must also be recognized as a common-mode failure point, especially with the increasing complexity of modern software systems. A 5G testbed will enable analysis of the vulnerabilities associated with power delivery, opportunities to design resilience and as a community we can contribute to the development, field validation and safety/cyber security verifications.

Initiative 1.A.iv.b: Cyber Security of Utility Support of 5G Capabilities

Utilities may augment 5G capabilities by providing suitable sites, power supplies and backhaul capacity more cost effectively in many areas than alternative operators. Examples may include:

- Joint ventures between utilities and telecommunications providers to deploy fiber backhaul connectivity.
- Provision of utility infrastructure for small cell sites, if safety, electricity reliability, and fair pole-attachment rates are considered.

- Facilitating power supplies to base station sites.
- Utilities providing 5G services to remote locations where they have a presence.
- Sharing spectrum with a commercial carrier so that the utility can lease the spectrum in areas where it is not being used by the commercial carrier.
- Disguising 5G antennas in utility infrastructure, again, where safe, feasible, and affordable. Cyber security of these modalities must be understood and managed.

Strategy 1.B: Uplift Cybersecurity Research Infrastructure.

CCI NoVa Node will expand shared research resources between institutions in the node, other nodes, and the Hub. Specific initiatives may include:

Initiative 1.B.i: 5G-enabled Test Beds

Development of 5G enabled physical test beds to support research and training in security of transportation, power, manufacturing, and communications systems.

Initiative 1.B.ii: Provide external community with access to research expertise across the node through the CCI NoVa Node website.

The website will be a place to showcase CCI NoVa Node research and CPSS R&D capabilities of industry and government partners as well as academic partners.

Initiative 1.B.iii: Stand up the The CCI Northern Virginia Node Living Cyber Innovation Lab.

The CCI NoVa Node Living Cyber Innovation Lab will include a 5G testbed for the study of cyber physical system security research, training and experiential learning. specific focus of the testbed will align with CCI NoVA Node strategic plan in multiple areas transportation, and power distribution, national defense. The Cyber Living Innovation Lab will include autonomous vehicle sensor platforms to study 5G performance and security vulnerabilities. These platforms will support Lidar, radar, stereo and night vision cameras that will be deployed on the NoVa Node's fleet of vehicles to simulate autonomous driving. The vehicles will be deployed throughout the Northern Virginia Node and may remain in residence at Node partners' institutions for periods of time to collect data. NoVa Node partners will leverage the NoVa Node 5G testbed in Arlington to analyze data, experiment, and develop new studies. The Cyber Living Innovation Lab will also include robotic platforms to evaluate 5G performance and security vulnerabilities including study of impact of 5G on the security of Industry 4.0, and smart manufacturing, and the vulnerability of the supporting power grid.

The Living Innovation Lab also supports the NoVa Node's Workforce Development Strategic Plan goal to: **Grow workforce-ready cybersecurity and cyberphysical system security talent to meet today's demands and tomorrow's economy: Provide experiential learning opportunities to students to enable them to apply knowledge, skills and abilities acquired in classroom to real-world cyber challenges.** The Cyber Living Innovation Lab will enable research a well as hands on experiential learning and will be open to all NoVa Node partners. An adjacent training facility will enable instruction of NoVa Node partners on the use of experimental equipment, including fleet of vehicles, radar, lidar and stereo and night vision cameras, sensors, data collection, data analytics and experimental design. Office space for NoVa Node faculty, other partner visitors and graduate student researchers to remain in residence for variable periods will be included. This facility will also enable instruction of cohorts of community college students and undergraduates incorporating hands on experiential exercises to elucidate classroom instruction on security of CPS, 5G, transportation networks, manufacturing, and power.

GOAL 2: ACCELERATE CYBER STARTUP CREATION AND TECHNOLOGY COMMERCIALIZATION

Strategy 2.A: Source/discover critical challenges from public and private sector to inform startups in region and attract Venture Capital (VC)

Initiative 2.A.i:

Deliver series of collider events with Science & Technology developers in federal government agencies and technology developers

Initiative 2.A.ii:

Deliver series of collider events with Science & Technology developers in private sector companies and technology developers

Strategy 2.B: Develop physical ecosystem in Northern Virginia to attract new cyber entities

Initiative 2.B.i:

Develop model for public-private partnerships to bring resources of industry, academia and government together, along with CCI resources, for management support of startup company development

Initiative 2.B.ii

Make affordable space available to startup companies by collocating them in premises of existing large companies who are willing to offer incubator space, and universities that provide incubator spaces in their academic buildings (e.g. George Mason, James Madison)

Initiative 2.B.iii

CCI NoVa Node serve as conduit for government and private entities to direct new technologies, not yet ready to launch as a company, to partner accelerators

Initiative 2.B.iv

Work with network of accelerators both inside and outside the region to widen VCs. Leverage resources, such as CCI grants, Virginia Small Business Financing Authority (VSBFA), Small Business Innovation Research (SBIR), Small Business Development Center (SBDC), Small Business Technology Transfer (STTR)) to provide seed funding for new cyber technologies.

Initiative 2.B.v

Scale existing programs and resources such as Innovation Commercialization Assistance Program (ICAP) and I Corp-style programs to expand impact.

Strategy 2.C: Develop next generation of cyber entrepreneurs

Initiative 2.C.i: CCI NoVa Node serve as clearinghouse of student opportunities to gain experience with entrepreneurship programs in Universities

For example, e.g.

i. Mason Summer Entrepreneurship Accelerator (https://startup.gmu.edu/entrepreneurial-programs/students/msea-mason-summer-entrepreneurship-accelerator),

ii. StartUpUMW (https://economicdevelopment.umw.edu/home/programs/student-entrepreneurship/),

iii. Shenandoah University Institute for Entrepreneurship Programs (https://www.su.edu/business/special-programs/institute-for-entrepreneurship/),

iv. James Madison University Venture Creation Accelerator (https://www.jmu.edu/cob/centers/center-for-entrepreneurship/students/venture-creation-accelerator.shtml),

v. Dual enrollment for high school students in entrepreneurship courses https://chantillyacademy.fcps.edu/academics/entrepreneurship).

Leverage NoVa Node Website to consolidate information.

Initiative 2.C.ii:

Develop female and minority entrepreneurs through outreach to non-profit organizations supporting cyber security, e.g. CCI NoVa Node co-host entrepreneurship events with organizations like Women in Technology, Historically Black Colleges and Universities (HBCUs), Women's Society of Cyber, et.al

Initiative 2.C.iii:

Develop a network of business leaders, mentors with experience in lean startup who are willing to counsel startups by partnering with non-profit organizations supporting cyber security, etc.

Goal 3: Grow workforce-ready cybersecurity and cyberphysical system security talent to meet today's demands and tomorrow's economy.

Strategy 3.A: Provide cyber experiential learning opportunities to students

Provide experiential learning opportunities to students (defined broadly) to enable them to apply knowledge, skills and abilities acquired in classroom to real-world cyber challenges. Experiential learning opportunities should span needs of entire student cycle. For example, middle/high school students practice basic computing and soft skills are reinforced, college/university level students practice specific cyber knowledge, skills and abilities, and experienced workforce reinforce advanced and emerging practices.

Initiative 3.A.i

Develop electronic clearinghouse of cyber internship and apprenticeship opportunities for students, support for matching, and incentives for their participation, e.g. competitive pay, credit (ties into the development of the website that we discussed that is seeded by NVRC to Mason CCI Node website and yr 2 of JP Morgan web effort and scaled to Formal Internship/Apprenticeship Portal)

Initiative 3.A.ii

Provide competitive hackathon (or challenge-athon) opportunities for varied levels (high school through higher-ed)

Initiative 3.A.iii

Provide physical testbed facility(s) to enable training (5G, IOT security) similar in concept of Virginia Cyber Range (virtual)

Initiative 3.A.iv

Provide experiential training opportunities that emphasize soft skills, e.g. team work, communications, personal conduct. A standard rubric to assess soft skills should be developed to help measure successfully mastered skills.

Strategy 3.B: Incentivize selection of cyber and cyber related education/training pathways (defined broadly)

Initiative 3.B.i

Provide scholarship for service or similar concept

Initiative 3.B.ii

Align (or document alignment) of academic curriculum (middle school, high school, college/university) with NICE Framework (https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework) and industry identified skills, knowledge and abilities to ensure direct connection between education pathway and job (Tech Pathway Campaign tool helps with this)

Initiative 3.B.iii

Scale region-wide communication plan (Tech Pathway campaign) to draw K-12 into cyber related education/training/career pathways.

Initiative 3.B.iv

Develop outreach plan to develop pipeline of diverse students including experiences, communications, marketing and financial support to ensure sustainable.

Strategy 3.C: Reduce cost of cyber education and training and time to degree completion

Initiative 3.C.i

Align industry certifications with credit bearing coursework and ensure credit transfer from dual enrollment, through community college to four-year institutions

Initiative 3.C.ii

Enable credit for prior-work (e.g. Veteran MOS) and ensure credit transfer between institutions

Strategy 3.D: Enable Scale (longer term)

Initiative 3.D.i

Call to industry to supply qualified adjunct instructors at all levels of educational pathway (high school through higher ed). Graduate PhD students may also serve as source of adjunct instructors.

Initiative 3.D.ii

Seek waiver for teachers, with proper training outside advanced degree in cybersecurity, to teach dual enrollment courses

Initiative 3.D.iii

Enable teacher training in cybersecurity to enable them to teach dual enrollment courses as well as high school foundational courses.

Initiative 3.D.iv

Staff to support Strategies 1-3

Goal 4: Build a collaborative Network

Strategy 4.A. Develop collaborative relationships within each Node

Initiative 4.A.i

Develop collaborative research opportunities with NoVa Node partners

Initiative 4.A.ii

Share results of CCI research through workshops, meet ups, communications

Initiative 4.A.iii

Scale ICAP Program across the Node

Initiative 4.A.iv

Include links to NoVa Node partner websites that provide internship and employment opportunities

Initiative 4.A.v

Provide physical testbed facility(s) to enable training (5G, IOT security) similar in concept of Virginia Cyber Range (virtual)

Strategy 4.B. Develop collaborative relationships between CCI Nodes

Initiative 4.B.i

Develop collaborative research opportunities with other CCI nodes

Initiative 4.B.ii

Share results of CCI research through workshops, meet ups, communications with other CCI Nodes

Initiative 4.B.iii

Scale ICAP Program across the Commonwealth

Initiative 4.B.iv

Include links to other Node websites that provide internship and employment opportunities

Initiative 4.B.v

Provide physical testbed facility(s) to enable training (5G, IOT security) similar in concept of Virginia Cyber Range (virtual)

Initiative 4.B.vi

Share communications and outreach plans developed in the NoVa Node with other Nodes.