Commonwealth Cyber Initiative Blueprint

December 1, 2018

TABLE OF CONTENTS

1 Executive Summary 3

2 CCI: A Call to Action 6

The CCI Imperative 6

The CCI Ecosystem, Building on Strength 7

A Collaborative Approach 8

Blueprint Partners 9

3 The CCI Opportunity 10

Virginia's IT Innovation Economy 10

Economic Diversification at the Intersection of Data, Autonomy, and Security 13

Cyber Research in the Commonwealth 14

Virginia's Cyber Workforce 16

Cyber Education in the Commonwealth 18

4 CCI Strategic Framework 19

CCI Mission and Vision 19

Goal 1: Build world-leading research and innovation capabilities 20

Goal 2: Help close the Commonwealth's cybersecurity workforce gap 27

5 CCI Implementation 34

Structure, Governance, and Node Certification 34

Budget 37

Timing 39

Continuous Improvement, Metrics, and Targets 40

Guidelines for Faculty Recruitment 43

6 Acknowledgements 44

7 Appendices 48

CCI Enabling Legislation 48

Faculty at Virginia Universities working on CPSS 50

EXECUTIVE SUMMARY

1

The Commonwealth Cyber Initiative (CCI) will create a Commonwealth-wide ecosystem of innovation excellence in cyberphysical systems (CPS) with an emphasis on trust and security. CCI will ensure Virginia is recognized as a global leader in secure CPS and in the digital economy more broadly for decades to come by supporting world-class research at the intersection of data, autonomy, and security; promoting technology commercialization and entrepreneurship; and preparing future generations of innovators and research leaders. CCI will build on Virginia's strong base of research excellence, its innovative and diverse higher education system, vibrant ecosystem of venture capital investment and high-growth firms, and unparalleled density of cybersecurity talent.

CCI must address two challenges, today's workforce gap, and tomorrow's new economy. They are different facets of the same problem and opportunity. To focus only on today's workforce challenge is to miss an opportunity to diversify the economy. Today's assessment is a look in the rear-view mirror. Conversely, to focus only on the future economy is to ignore the fact that the basis for that economy is threatened by the workforce gap.

CCI is a highly-connected Network that engages of institutions of higher education, industry, and government, along with non-governmental and economic development organizations. It will connect Regional Nodes across the Commonwealth, each led by an institution of higher education. Regional Nodes will be vibrant centers of research, learning, and innovation tailored to their local ecosystem. To ensure success, CCI Regional Nodes will be certified by VRIC consistent with the commitment of Regional Node partners to the goals of the initiative.

The Hub, anchored by Virginia Tech and located in Northern Virginia, will enable world-class research focused on cybersecurity. By hosting faculty from CCI Network institutions, industry partners, and entrepreneurship programs, the CCI Hub will provide a center of mass for the cybersecurity innovation ecosystem across the Network, acting as a beacon to draw talent and partners to the Commonwealth.

The Hub will also coordinate the Network, strengthening connectivity and programs to build and align assets across Virginia, amplifying the efforts already underway and providing a one-stop access point to CCI resources for all stakeholders, current and future. To achieve its goals, CCI will both develop new programs and promote, amplify, align, and grow existing efforts across Virginia. CCI's success relies on the active collaboration of institutions of higher education across the Commonwealth, contributing their experience, ideas, and expertise. The CCI Network will create an ecosystem that is greater than the sum of its parts.

CCI will build and a research alliance across the Network to build a Commonwealth-wide cyber innovation ecosystem, support curriculum alignment for more seamless credit transfers across the Commonwealth, cultivate holistic relationships with industry and government partners to support research, education, and experiential learning across the Commonwealth; and collect of market research and performance data, supporting strategic decision-making and continuous performance improvement.

CHANGE OF TERMINOLOGY

During the collaborative Blueprint development process, participants agreed that a Regional Node model was a more appropriate way to characterize the Commonwealth-wide Network than using the phrase "spokes." This change is consistent with the purpose of the CCI enabling legislation. Consistent with the budget language, the "Hub" will serve not only as coordinator and central connector of the Nodes, it will also lead cyber, workforce, and education for the CCI.

EXECUTIVE SUMMARY

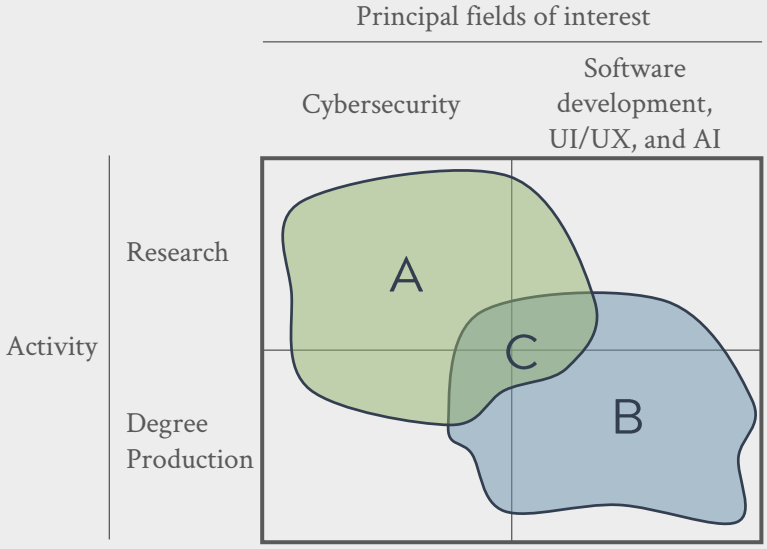
1

Key activities include:

- **Cyberphysical System Security (CPSS) Research**: CPS and the internet of things promise to enhance the quality of life in many ways, but require advances in security and trust to ensure robust, safe, and widespread adoption and impact. This includes world-class research teams at the Hub and across the Network focused on the next-generation communication technologies that will support the internet of things, as well as machine learning and artificial intelligence for cybersecurity. Through a Network-wide research alliance, the team will partner with and host CCI-aligned researchers from institutions across the Commonwealth, bolstering CCI Network ties and enhancing synergies across the Nodes.
- **Entrepreneurial Ecosystem**: The CCI Network is committed to ensuring that research outcomes make their way to market quickly and effectively. CCI investments will grow and diversify the Virginia cyber economy Commonwealth-wide by promoting the commercialization of CPSS products and launching cyber-focused startups. The CCI Hub will support entrepreneurship across the Network by providing access to venture capital and supporting startups. CCI will support technology de-risking through approaches like proof-of-concept grants. In addition, Nodes will promote CPSS research and entrepreneurship in their regional ecosystems.

AMAZON HQ2

On November 13, 2018, Amazon chose Virginia to house a new headquarters. One of Virginia's commitments related to HQ2 is a tech-talent pipeline initiative. CCI and the proposed tech-talent pipeline initiative are different but complementary. The graphic below was presented to the Virginia House Appropriations Committee.



A **Commonwealth Cyber Initiative** will bolster the cybersecurity talent pool primarily through investments in Virginia's research capabilities (e.g., labs, faculty) and commercialization efforts.

B **The Tech-talent Pipeline Initiative** will increase the number of graduates across a variety of tech-related fields (e.g., software development, UI/UX, and AI) prepared to excel in the tech sector; some research investment will be necessary but will not be the primary objective

C The two efforts have **different objectives though some overlap** (e.g., research and faculty investments) will occur.

EXECUTIVE SUMMARY

1

- **Co-Op 2.0 Portal**: To ensure that Virginia students are fully prepared to enter the innovation workforce upon graduation, the CCI Network will promote and support opportunities for long-term and year-round experiential learning in ways that do not prolong student time-to-degree. These longer-term relationships increase value for both stakeholder groups. CCI will support the distance learning, flexible educational schedules, and industry partnerships required to establish and scale these experiences across the Commonwealth. CCI funding will be made available for matching industry investment in student stipends.

The 2018-2020 Virginia State Budget invests $25 million in CCI. This appropriation includes $10 million to scale the initiative and recruit faculty both the Hub and Node sites. An additional $10 million is provided to establish the Hub, including research faculty, entrepreneurship programs, and student internships. Finally, $5 million is available for renovations, space enhancements, and equipment.

CCI's success will be measured by well-defined output indicators (see table). CCI will also produce real outcomes for the Commonwealth, such as student employment in cyber fields in Virginia industry, patent licensing, and venture capital invested in spin-outs.

To achieve these outcomes, CCI recommends an additional $40 million in funds to further scale the Hub, pilot new programs to scale degree production, and recruit scholars and researchers across the Commonwealth. The CCI Network should be sustained by a $28 million annual investment in research and educational faculty support, Co-Op 2.0 support, and other Network programs. These funds will be leveraged to grow a combination of philanthropy, industry investment, and sponsored research programs totaling over $20 million for the initial investments and growing to $35 million annually at steady state.

	Baseline	Δ FY2022	Δ FY2026
FACULTY PARTICIPATING ACROSS NETWORK	200	25	65
ANNUAL SCHOLARLY PUBLICATIONS ACROSS NETWORK	800	100	300
ANNUAL COMPETITIVE RESEARCH EXPENDITURES ACROSS NETWORK	(TBD)	$10 M	$30 M+
CUMULATIVE COMPANIES LAUNCHED	(TBD)	3	10
ANNUAL DEGREE PRODUCTION IN CYBER-FOCUSED DEGREES†	450	150	450

CCI: A CALL TO ACTION

2

THE CCI IMPERATIVE

Virginia is uniquely positioned to demonstrate global leadership in secure CPS, including underlying cybersecurity technologies. The Commonwealth's strengths include an unrivaled density of IT talent, industry, and venture capital (VC), creating a highly fertile environment for innovation and tech-based economic growth.

Today, an overwhelming majority of Virginia's firms are focused on providing IT cybersecurity services to the federal government. This creates a high demand for IT workers and subjects the Virginia economy to federal budget cycles. To build a high-growth, resilient economy, Virginia must become a leader in consumer- and commercially-facing cybersecurity for technologies at the frontier.

Recognizing the strategic importance of economic diversification, the 2018-2020 Virginia State Budget (the Biennium budget, see Appendices) established the Commonwealth Cyber Initiative (CCI).

CCI is designed to connect public institutions of higher education across Virginia with industry partners to develop an ecosystem of research, innovation, commercialization, and learning to propel Virginia into a position of leadership in cybersecurity for the growing Internet of Things. A Network composed of a Hub, led by Virginia Tech, and Regional Nodes located around the Commonwealth. The Nodes will be led by institutions of higher education, certified by the VRIC. The Biennium budget includes $25 million over two years for CCI.

Virginia Tech President Tim Sands addresses the Commonwealth Cyber Initiative Blueprint Advisory Council, September 21, 2018

Out of this appropriation, $10 million is provided in fiscal year (FY) 2020 to scale the initiative and provide matching funds for faculty recruiting at both the Hub and Node sites. An additional $10 million is provided in FY2020 for the leasing of space and establishment of the Hub by the leading institution and for the establishment of research faculty, entrepreneurship programs, student internships and educational programming, and operations of the Hub. Finally, $5 million is available in FY2019 for renovations, space enhancements, and equipment.

CCI is focused on breakthrough research and innovation in CPSS to diversify Virginia's economy and preparing for the continued digital evolution of society. It will also seek to help develop a talented cybersecurity workforce, addressing a key challenge for Virginia's current economy.

Recognizing the Commonwealth's increasing need for talent development across data science and technology, science and engineering, health, and education, the higher education package in the Biennium budget also included separate funds targeted to degree production in high-demand fields. This appropriation of $28.4 million across Virginia's public institutions of higher education will support 880 new degrees per year in those areas.

The Biennium budget requires Virginia Tech to develop a Blueprint for establishing CCI, to be delivered to VRIC by December 1, 2018. This Blueprint describes how to best achieve the vision set out for CCI. Given the scope of the opportunity and the need for sustained effort, the appropriation for the current biennium will be sufficient only to seed CCI. Additional one-time resources along with a base appropriation will be necessary in subsequent biennia to realize the vision for CCI.

CCI: A CALL TO ACTION

2

THE CCI ECOSYSTEM

CCI exists in a larger ecosystem of programs, platforms, and pipelines that will contribute to its long-term success. While they are outside of the scope set for CCI, it is important to recognize their importance to Virginia's cybersecurity ecosystem.

The Commonwealth's cybersecurity talent pipeline has many opportunities for growth before students even enter the higher education system. Early childhood education lays the foundation for a lifetime of learning and success in the digital economy.

Interest in and preparedness for a career in cybersecurity starts early. Cybersecurity principles and technologies must be incorporated into the curriculum throughout the education system. Increased partnerships with the business community throughout the education system will support robust talent development.

In addition, expanded opportunities and support for dual-enrollment between Virginia's K-12 education system to higher education would strengthen the talent pipeline for years to come. By preparing students with targeted cybersecurity courses in high school, time to degree and educational debt can be decreased, giving students a better shot at success. Challenges include hiring and training certified dual-enrollment teachers, as well as enabling efficient articulation with multiple school districts.

Finally, cybersecurity is an all-hands-on-deck challenge. An intentional approach to diversifying the talent pipeline through special efforts to encourage women and minorities to consider a career in cybersecurity will be necessary to produce enough potential workers to meet industry's cybersecurity needs. In addition, cybersecurity permeates every industry and every career. Every student must be prepared to contribute productively and securely to the digital economy.

BUILDING ON EXISTING STRENGTH

CCI's potential for success is bolstered by the dynamic, innovative, and growing cybersecurity research, education, and talent development programs across the Commonwealth and capital region. The CCI Blueprint development process highlighted the many programs that exist across Virginia that can be leveraged, amplified, and coordinated through the CCI Network. By building on the best practices of programs across Virginia, CCI will enable a system that is greater than the sum of its parts. The CCI Network will be strongest if it includes the widest possible array of universities and programs.

Some of those programs are highlighted throughout the document in grey boxes. There are too many to describe comprehensively in this Blueprint. One of the first opportunities for CCI is to build a library of available programs across the Commonwealth.

In addition, leadership in cybersecurity requires high levels of security within participating institutions' IT systems. CCI Nodes must be committed to continuing to improve their IT security posture.

APPRENTICESHIP PROGRAMS

Companies across the Commonwealth and the nation are actively supporting the development of cyber talent. Amazon Web Services' Apprenticeship program for members of the military community provides intensive full-time training, followed by paid on-the-job training and an opportunity for a full-time position. Telos Corporation recently initiated a similar program, hiring veterans at 60 percent of base pay during a full-time training period prior to employment. Small companies are also participating, with Peregrine Technical Solutions LLC offering the Commonwealth's first Department of Labor certified apprenticeship in cybersecurity.

Efforts like these represent real investment by companies in Virginia's cyber workforce, and present an opportunity to accelerate learning, build a sticky talent pipeline, and overcome persistent challenges in gaining necessary security clearances.

CCI: A CALL TO ACTION

2

A COLLABORATIVE APPROACH

To develop this Blueprint, Virginia Tech convened an Advisory Council of more than 80 participants from universities and community colleges across the Commonwealth, as well as representatives from industry, government, non-profits, and other non-governmental organizations. A fifteen-person executive committee was established to provide high-level guidance and advice. Four working groups with designated subject matter expertise from institutions on the Advisory Council, co-chaired by members of the executive committee and designees from Virginia Tech, were convened. The working groups focused on Research and Technology Commercialization, Educational Programs and Experiential Learning, Partnerships and Investment, and Finance and Government Relations.

The cadence of meetings was set according to each group. For example, the Research and Technology Commercialization working group met in person for a kick-off event, and then held subsequent conference calls on three focus areas.

The Executive Committee met in person in August and September, and then held three conference calls throughout October.

The full Advisory council met three times: at a kick-off conference call in July, a day-long retreat in September, and a half-day capstone meeting in November.

BLUEPRINT TIMELINE

CCI: A CALL TO ACTION

2

CCI BLUEPRINT PARTNERS

Representatives from the following organizations participated in Blueprint development.

Business and Industry

- 10Pearls
- Attain LLC
- Center for Innovative Technology
- Dominion Energy
- G2 Ops, Inc.
- Hunch Analytics
- MACH37
- McGuireWoods Consulting LLC
- Northrop Grumman
- Opportunity Inc.
- Peregrine Technical Solutions, LLC
- Sentara Healthcare
- Siemens Energy
- Simone Acha Consulting
- Tangible Security
- TEConomy Partners LLC
- Telos Corporation
- The Aerospace Corporation
- The MITRE Corporation
- United Bank

Higher Education

- Christopher Newport University
- George Mason University
- James Madison University
- Longwood University
- Marymount University
- Norfolk State University
- Northern Virginia Community College
- Old Dominion University
- Radford University
- Richard Bland College
- University of Mary Washington
- University of Virginia
- University of Virginia, College at Wise
- Virginia Commonwealth University
- Virginia Community College System
- Virginia Military Institute
- Virginia State University
- Virginia Tech
- William and Mary

Government and Non-Governmental Organizations

- Business Higher Education Forum
- Chief Workforce Development Advisor to Governor Northam
- GO Virginia
- Greater Washington Partnership
- Northern Virginia Technology Council
- State Council of Higher Education for Virginia
- Virginia Economic Development Partnership
- Virginia Research Investment Committee
- Virginia Space Grant Consortium

CCI Blueprint Development Participants at the Advisory Council Retreat
Clockwise from top left:

Peter Hesse (10 Pearls), Sharon Simmons (JMU), Leigh Armistead (Peregrine Technical Solutions)

Liza Wilson-Durante (GMU), Cyril Clarke (VT), Brian Payne (ODU)

John Wood (Telos Corporation), Aurelia Williams (NSU)

Melur Ramasubramanian (UVA), Cyril Clarke (VT)

THE CCI OPPORTUNITY

3

VIRGINIA'S IT INNOVATION ECONOMY

Virginia is well positioned to be a global leader in CPSS. It has a baseline of economic conditions primed for growth. For example, Virginia ranked fourth in the Information Technology and Innovation Foundation (ITIF)'s 2017 State New Economy Index. Virginia's stature is rising, having moved up three places since 2014 in that index, which is based on twenty five indicators across five areas (knowledge jobs, globalization, economic dynamism, digital economy, and innovation capacity).

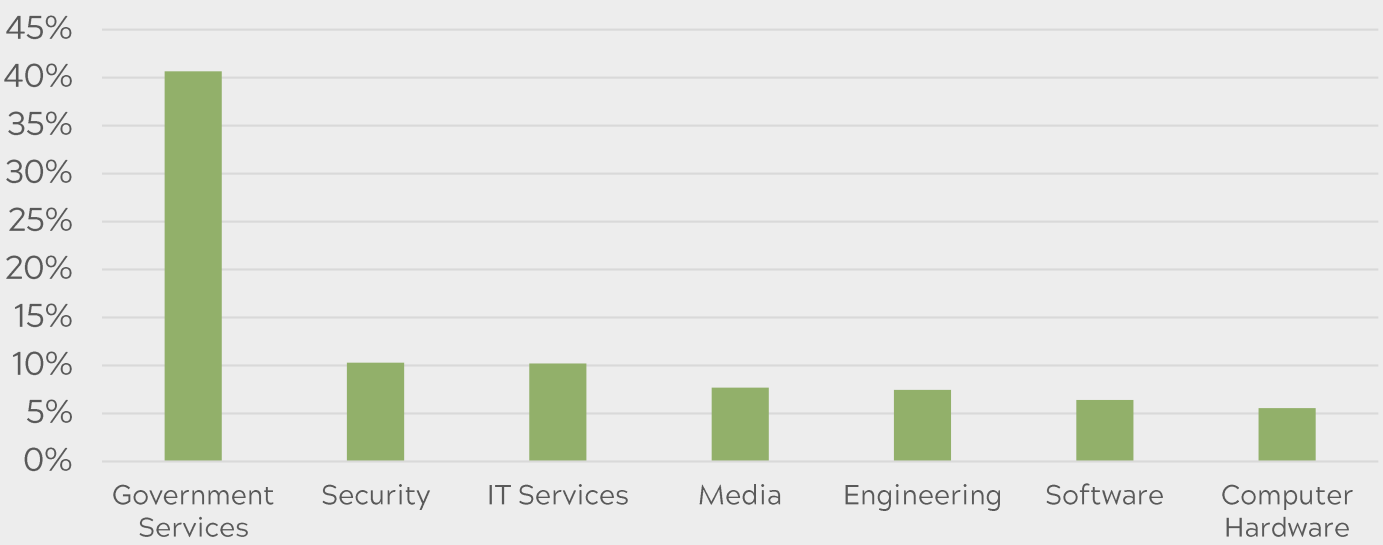
Virginia has exceptional strength in IT services and software across many of the indicators included in ITIF's analysis. For example, Virginia ranks highest for concentration of high-growth firms, based on the INC 5000 database. While many of those firms are in the government services sector, Virginia has more than its fair share of high-growth companies in IT services and software.

Another indicator of innovation and potential for economic growth is VC activity. A 2016 analysis by Martin Prosperity of VC clusters across the United States found high concentration of VC activity in IT services and software in the national capital region.

This highly productive economic cluster in IT services, software, and security will serve as a substantive foundation upon which to build a world-leading research and education center-of-mass in CPSS technologies.

In addition to this economic activity in IT, other indicators of high-growth potential include a highly educated workforce (Virginia is sixth in the nation, and the DC region ranks second). In addition, Virginia ranks second in density of cybersecurity jobs (exceeded only by DC), with four times the national average.

There is also a high level of research and development (R&D) in Virginia. With about $10 billion in R&D expenditures, Virginia ranks 13th in the nation.



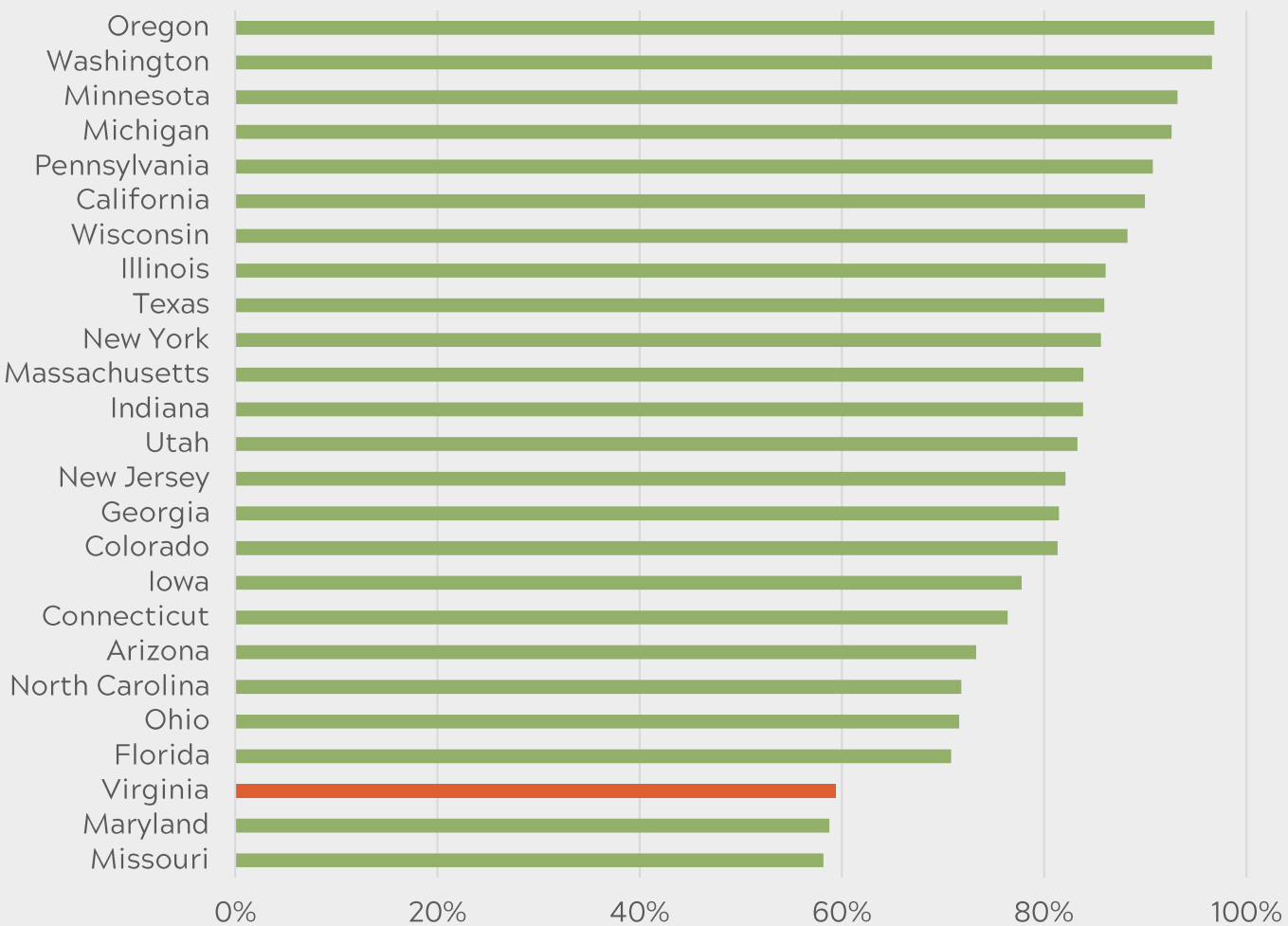
Virginia's share of high-growth companies across sectors where Virginia share is >5%. Virginia has nearly 40% of U.S. high-growth firms in the government services sector. Data from 2017 INC 5000 survey

THE CCI OPPORTUNITY

3

While Virginia's total R&D expenditures sound impressive, they are just slightly better than average. Virginia ranks 21st in the nation in research dollars as a percentage of gross domestic product (GDP). Furthermore, Virginia's research funding is overly dependent on the federal government: $4.6 billion spent on R&D in the Commonwealth in 2015 was across its federal intramural labs and federally funded R&D centers and almost a third of Virginia's industry research was through federal research awards and contracts—both are four times the national average.

According to the National Science Foundation, Virginia ranks 23rd for R&D performed by industry, slipping to 31st when normalizing to Virginia's GDP. Of that research performed by industry, others (mostly the federal government) pay for 40 percent.



Percentage of research performed by industry that is paid for by the company. Balance of research funding is paid for by others - principally the federal government.
Represents the 25 states with the largest industry R&D expenditures.
Data from National Center for Science and Engineering Statistics .

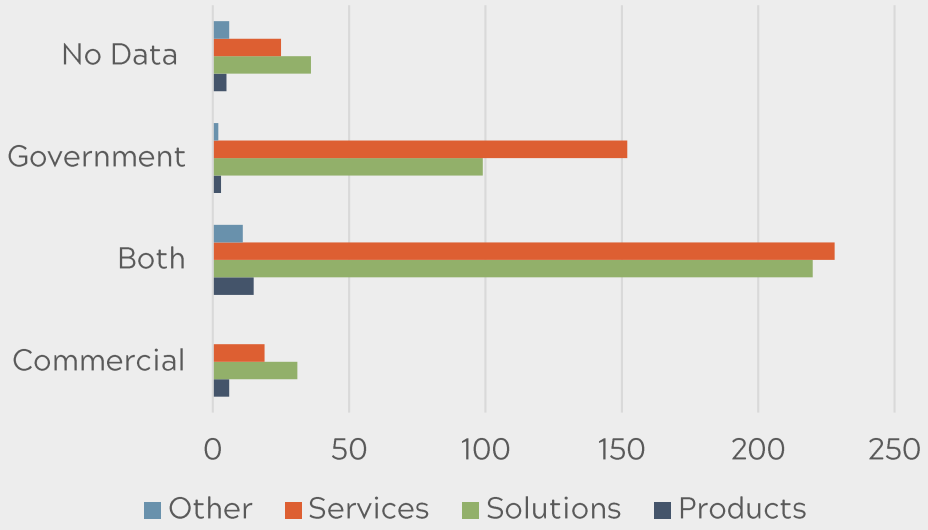
THE CCI OPPORTUNITY

3

A 2017 study showed that of the 858 cybersecurity companies in the capital region, more than half served only the federal government, while 6.4 percent served only the commercial sector. This focus on the federal government is not surprising, given the density of federal agencies in the region. It creates the economic risk associated with downturns in federal spending.

This focus on federal clients also shapes the business models of cybersecurity companies in the region. Only five percent of the firms had a product focus, while nearly 50 percent provided services, and the remainder offered hybrid product-service solutions. The focus on services, which is highly dependent on trained workers, limits the potential growth of the firms and puts additional pressure on the local workforce.

CCI seeks to diversify the Virginia cyber economy by promoting commercialization of next generation CPSS technologies, and by providing a locus of investment and partnerships in research and innovation.



Client and business focus of capital-region cybersecurity firms, by client focus and business focus. Cybersecurity firms in the capital region have a strong focus on providing services or solutions for the federal government. Data from http://www.tandemnsi.com/wp-content/uploads/2017/04/Tandem-Kogod-Report.pdf

THE CCI OPPORTUNITY

3

ECONOMIC DIVERSIFICATION AT THE INTERSECTION OF DATA, AUTONOMY, AND SECURITY

The internet of things (IoT) is fundamentally changing the DNA of the Internet. Over the past decade, we saw the emergence of the social-mobile Internet, which transformed the way we interact with data and each other. The next decade promises transformation on a similar scale, with new technologies like 5G and edge computing transforming the global information and communication technology (ICT) ecosystem into a malleable, virtualized fabric designed to support most any imaginable service.

The economic opportunity associated with IoT is immense. With applications for everything from manufacturing to transportation, from devices in the home to devices in the hospital, with critical infrastructure like energy and defense, nearly every sector of the economy will be affected by IoT. Because the scale is so large and the opportunity so diverse, projecting the economic impact is difficult. The Greater Washington Partnership (GWP) Technology Report states that the global market growth for IoT is 30 percent. Bain & Company predicts that the IoT and analytics market will grow from $235 billion in 2017 to $521 billion in 2021. McKinsey & Company estimates that IoT could have an economic impact of $3.9-11 trillion in 2025.

Such major transformations require new tools to combat existing cybersecurity threats, as well as new threats that will emerge over time. As society invents the IoT future, we must put significant effort into ensuring the security and integrity of enabling infrastructure, building privacy-native ways of handling data, and creating science to cope with questions of security for the artificial intelligence (AI) algorithms that will orchestrate the IoT. In fact, security for IoT has been cited as the primary concern for enterprises and customers alike. Gartner, Inc. predicts that spending on security for IoT could grow from just over $900 million in 2016 to over $3 billion in 2021.

Ubiquitous connectivity and computing, enabled by mobile broadband and cloud computing, are motivating everything to be connected, from home appliances to automobiles. Cloud-based data analytics, orchestration, and collaboration are enabling entirely new ways of interacting with technology and society. However, many of these newly-connected devices, like those in energy infrastructure and transportation systems, have safety-critical functions. Additionally, these devices often operate with design lifetimes of 20 or more years, making them fundamentally different than the phones and apps that fueled the last phase of Internet growth.

Many predict that the next generation of wireless communications technologies (5G) will accelerate the promise, and the challenges, of security for the IoT. With low latency and energy-smart devices that bring computing from core servers to the devices at the edge of the network, 5G is aligned with many visions of IoT in the future. Communications companies from Verizon to Cisco to Ford are betting on this future, making large investments in research, demonstration, and infrastructure deployment. Given CCI's underlying goal of growing and diversifying the economy, IoT security and its enabling technologies is an outstanding focus.

However, the IoT panacea faces complex risks. The cybersecurity and consumer trust challenges may be too difficult to overcome. The mismatch between technology innovation cycles in the ICT sector compared with those in the energy, transportation, and manufacturing infrastructure that hold the greatest promise for IoT may prove too challenging.

These are exactly the reasons for investment in a world-leading core of research expertise in Virginia at the intersection of security, autonomy, and data. The opportunities to grow and diversify the Commonwealth's economy are immense and the research field is not yet too crowded.

THE CCI OPPORTUNITY

3

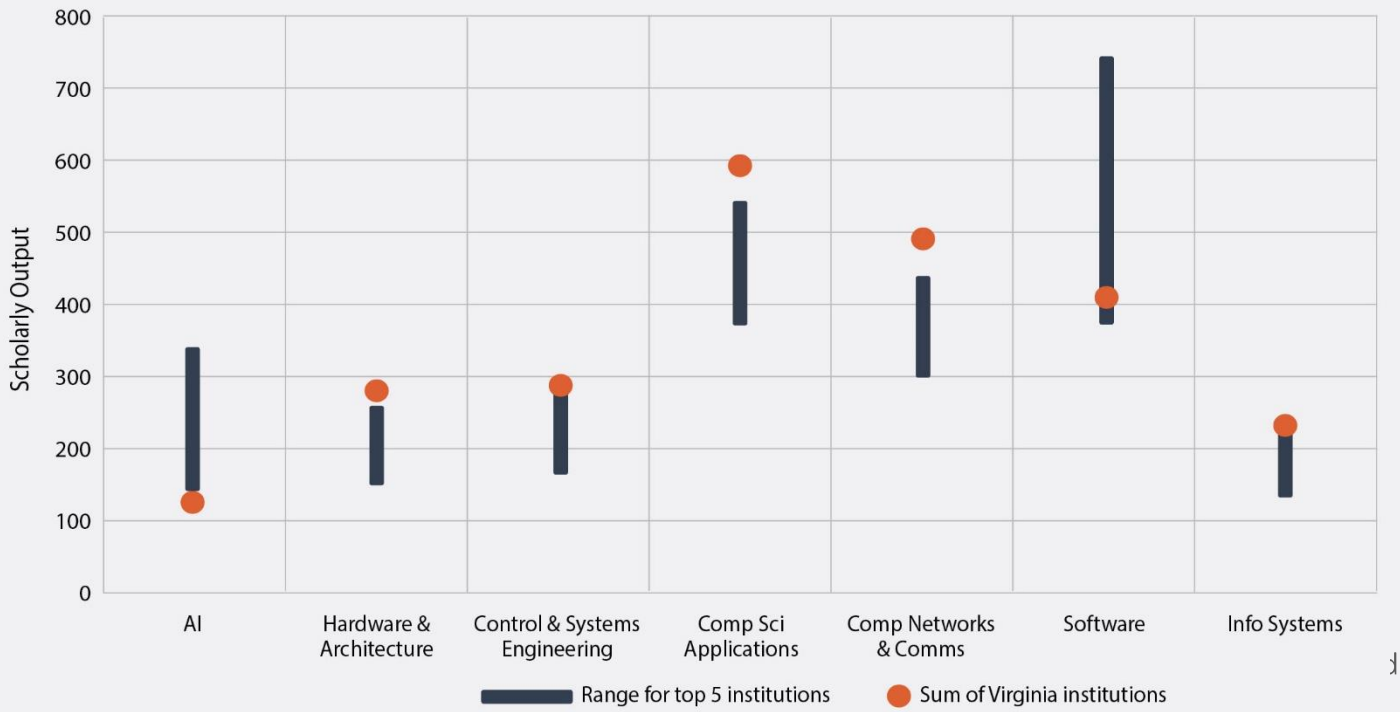
CPSS RESEARCH IN THE COMMONWEALTH

As described in the 2018 TEConomy report commissioned by VRIC, CPSS is one of four areas where Virginia has particular research and innovation opportunity. However, Virginia universities generally do not yet have leading research programs in fields related to CPSS. According to an analysis of peer-reviewed publications, Virginia has four public universities ranked in the top 100 U.S. entities by volume of scholarly output (e.g., peer-reviewed publications and conference proceedings) across fields such as software, information systems, computer networks and communications, computer science applications, control and systems engineering, and AI. Across these seven fields, the mean ranking of Virginia's ranked universities is 40. One university is in the top 15 in three of these fields and in the top 25 in five, and a second is in the top 30 in one field.

While Virginia institutions do not have national leadership in any of these areas, added together, they outperform leaders. The sum of Virginia's scholarly output outpaces the top publishing institution in most CPSS-related fields.

In addition to this strong base, every Virginia institution of higher education has hired research-active faculty in related fields in the past two years, a measure of Virginia's dedication to this area.

To be a world leader in CPSS, Virginia must augment its research capability. To this end, CCI will establish a critical mass of world-class principal investigators at the Hub with researchers across the Regional Nodes in a richly connected network that partners with industry on emerging socio-technical challenges.



includes peer-reviewed journal articles, reviews, books, conference proceedings, etc. The sum of the scholarly output of Virginia's ranked public universities is greater than the #1 ranked university in all fields except AI and software.

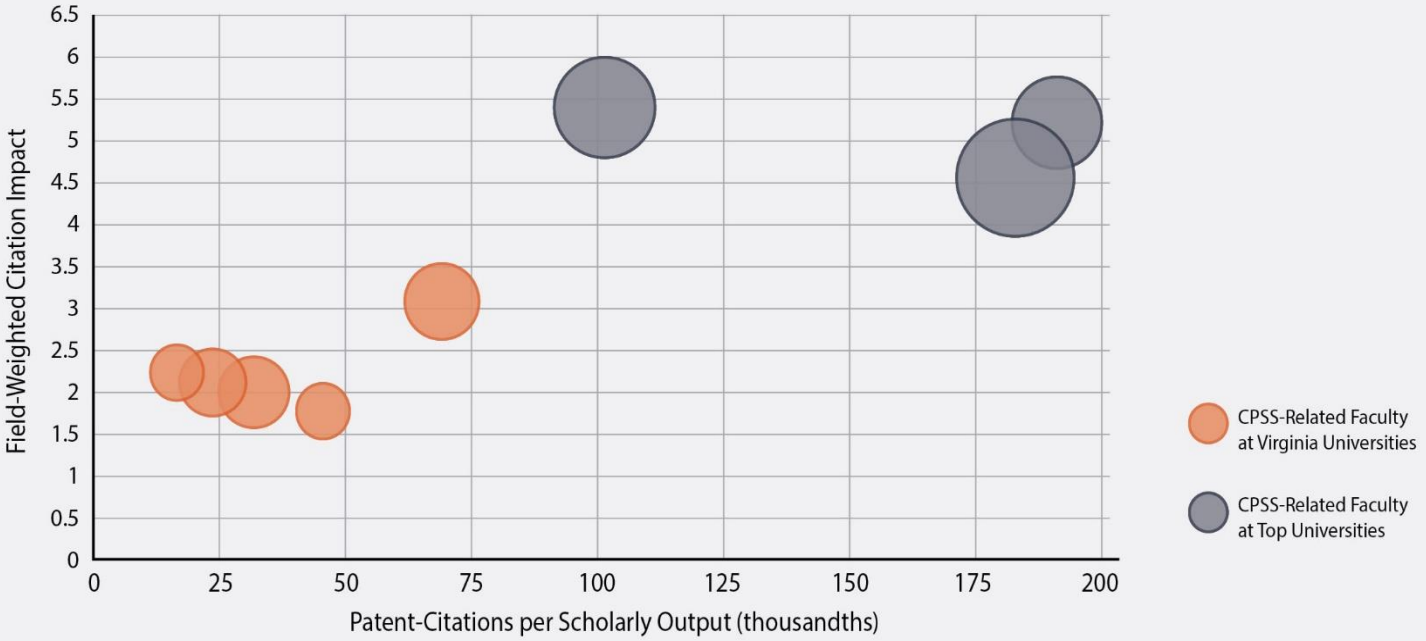
THE CCI OPPORTUNITY

3

During CCI Blueprint development, universities on the advisory council identified faculty with expertise related to CPSS (see Appendix). The chart below shows three measures of the collaborative and innovative quality of the scholarly outputs of faculty at Virginia universities compared to leading CPSS research groups at Carnegie Mellon, Stanford, and the University of Michigan.

Those research groups—which comprise 10-15 faculty each embedded in highly-ranked research ecosystems—perform research that is far more highly cited with a higher percentage of industry collaborators than Virginia's faculty. That influence, industry engagement, and innovation is an ambition for CCI.

There is intense competition for leadership across many broad cyber fields. For example, Massachusetts Institute of Technology recently announced a $1 billion investment in a new college focused on AI. Virginia's best approach to internationally-recognized leadership and a robust innovation ecosystem is to focus on one area of high technical and economic potential: CPSS.



Three measures of the collaborative and innovation quality of research outputs from Virginia CPSS-related faculty (orange), compared to leading research groups at Carnegie Mellon, Stanford, and the University of Michigan (grey).

Field-weighted citation impact (y-axis): number of citations normalized to field, journal, and year. Larger numbers indicate greater scholarly influence.

Patent-citations per scholarly output (x-axis): number of times publications are cited by patents, normalized to the volume of publications. Larger numbers indicate greater innovative influence.

Academic-Corporate Collaboration % (bubble size): percentage of publications with a corporate partner. Larger size indicates more frequent collaborations with industry.

All three indicators are normalized to volume of scholarly output because research groups on chart include very different numbers of faculty.

THE CCI OPPORTUNITY

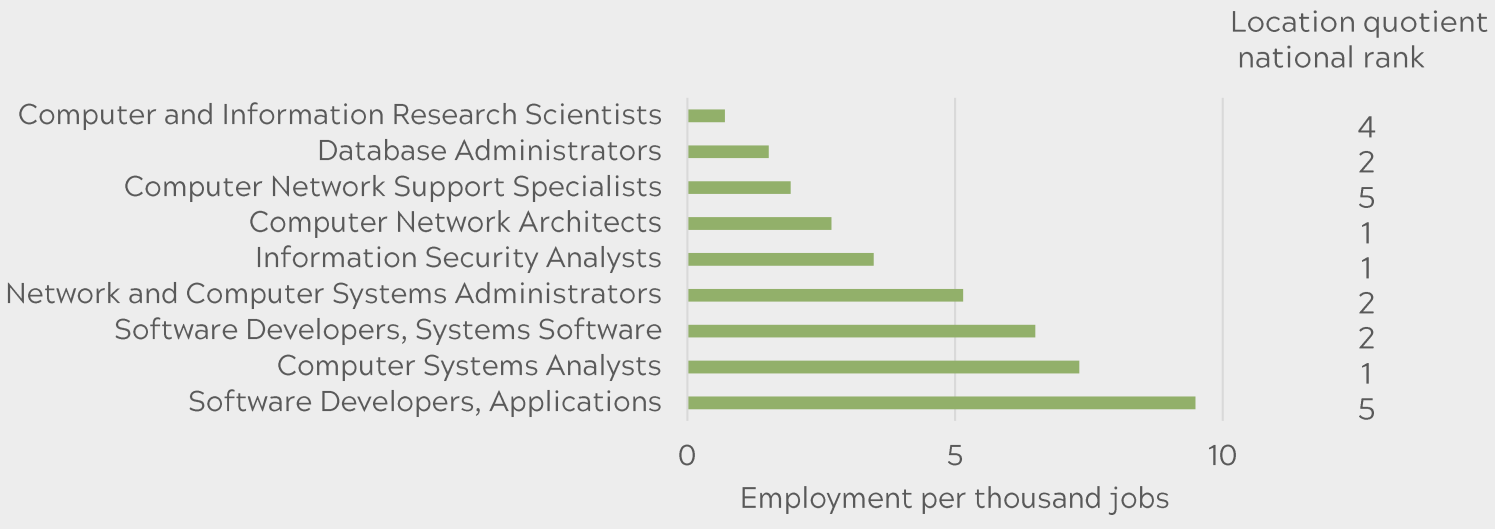
3

VIRGINIA'S CYBERSECURITY WORKFORCE

No other state has a higher concentration of cybersecurity workers than Virginia. According to the Cyberseek tool, a product of the National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE), Virginia's concentration of cybersecurity-related jobs is four times the national average.

According to the Bureau of Labor Statistics, Virginia ranks in the top five states in terms of most concentrated labor force across a number of computer and IT-related occupations—those occupations account for nearly four percent of Virginia's jobs.

However, beneath this incredible concentration and breadth of the cyber workforce lies a challenge. According to Cyberseek, from mid-2017 to mid-2018, employers posted more than 33 thousand jobs in cybersecurity-related fields. That is nearly half of the total employed cybersecurity workforce in Virginia.



Employment per thousand jobs and location quotient national rank. Virginia employment data from May 2017, according to the Bureau of Labor Statistics.

A note on the difficulty of obtaining high-quality, high-fidelity data on the cybersecurity workforce and education: the cyber workforce gap has long been acknowledged and studied by several groups. In the capital region alone, the GWP and the Business Higher Education Forum (BHEF) have examined the shape and scope of the workforce challenge. The scope of the national challenge is so great that NICE, a federal program, was established in 2014 to convene stakeholders to address it.

There is not a single, agreed-upon definition of cybersecurity, let alone the cybersecurity workforce. The federal databases for labor statistics and education statistics use codes that do not uniquely map to cybersecurity. NICE has produced a framework for cyber education, but that has not yet been universally adopted by employers or educators. Analyses that rely on job posting data are prone to errors caused by jobs posted for government contracts never awarded, among other errors.

And, of course, the workforce is always changing. Cybersecurity is in many ways uniquely dynamic, with threats and technologies evolving more quickly than federal databases and bureaucratic definitions can keep up.

THE CCI OPPORTUNITY

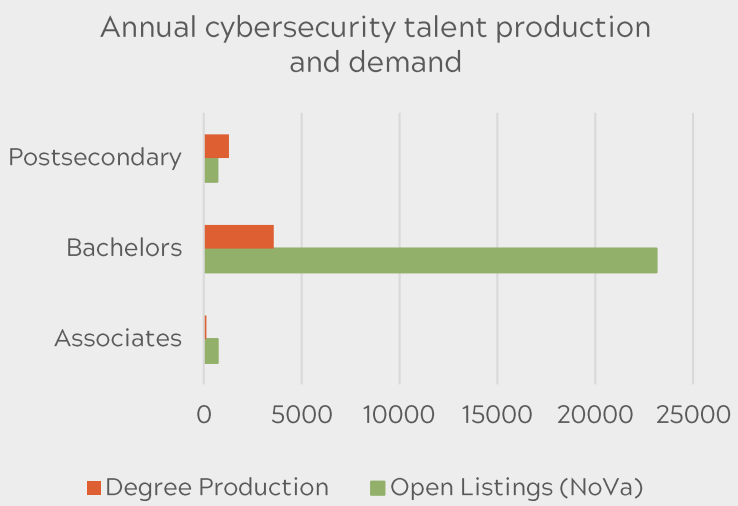
3

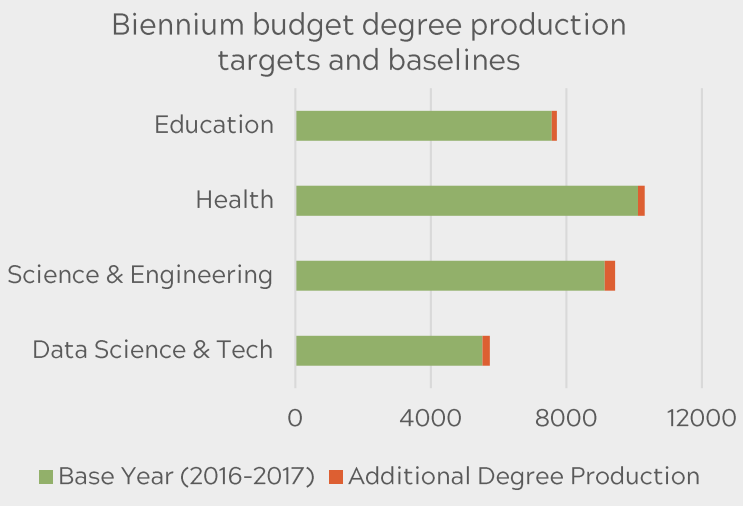
Nearly 90 percent of postings that had specified degree requirements require at least a bachelor's degree. According to a call for data performed by the Educational Programs and Experiential Learning working group, Virginia public and private institutions of higher education produced just over 4,800 degrees—BS or above—with some component related to cybersecurity fields in the past year. About 860 of those degrees are in cybersecurity-focused fields. At that rate, even if every graduate stayed in the Commonwealth, it would take more than five years to fill Virginia's open positions.

Recognizing the need for increased talent development in high-demand fields, the Virginia General Assembly provided $28.4 million in the Biennium budget to public institutions of higher education for degree production in data science and technology, science and engineering, health, and education. The target degree production is 880 degrees—about $32,274 per degree—on top of more than 32,000 degrees produced annually in those fields.

Virginia's employers need an experienced workforce. Only one in nine cybersecurity-related job postings is for someone with less than three years of experience. In fact, Virginia institutions of higher education produce more students with bachelor's degrees each year than employers wish to hire. That experience gap must be filled with meaningful experiential learning opportunities.

It is important to note that many of these postings require specialized certificates and clearances that are outside the typical higher education portfolio. Because of the high concentration of government contractors in Virginia, more than one third of jobs posted require a security clearance. Others require cybersecurity certifications offered by industry associations (like the Certified Information Systems Security Professional from ISACA or the CompTIA Security+), specialized offerings (like the Global Information Assurance Certification), or vendor-specific certifications (offered by Microsoft, Cisco, Red Hat, Amazon, and others).





Left: Number of graduates (orange) and job postings (green) by educational attainment. Number of graduates is self-reported data on cybersecurity-related degree production collected by Educational Programs and Experiential Learning working group. Open Listings is minimum educational attainment for postings from Sept '17 to Aug '18 in Northern Virginia, analysis of Burning Glass data by NVCC.

Right: Number of target degrees produced (orange) compared to base-year degree completion (green) targeted in year two of the Biennium budget. Data sciences and technology degrees are related to CCI.

THE CCI OPPORTUNITY

3

CYBER EDUCATION IN THE COMMONWEALTH

Virginia's institutions of higher education are extraordinarily forward-leaning and innovative in preparing their students for jobs in cybersecurity. Every participating institution is looking for ways to increase the number of degrees awarded in cyber-related fields, to incorporate cybersecurity elements into a wide variety of degrees, to diversify their student populations in this area, and to partner with other institutions to achieve these goals. The success of CCI will rely on convening, coordinating, and sharing the best practices of these programs. CCI should not duplicate, but amplify, these efforts.

The CCI program as appropriated will not directly fund enrollment growth or degree production. That is not because it is not a worthy goal—preparing Virginia's students to be successful in the workforce, and supplying Virginia's employers with the talent they need is critical to the economy. The gap is simply too large to reasonably fill through additional undergraduate degree production alone.

CENTERS OF ACADEMIC EXCELLENCE

The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cyber defense and producing professionals with cyber defense expertise.

NSA also sponsors a CAE in Cyber Operations program. The CAE-CO program is a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.

Sixteen Virginia institutions of higher education have designations across the two-year education (CAE-2Y), baccalaureate/graduate education (CAE-CDE), and research (CAE-R) categories. Further, NVCC is a CAE National Resource Center for Peer Review. Virginia Tech is a designated CAE-CO.

CAE-CDE

- ECPI University
- George Mason University
- Hampton University
- James Madison University
- Liberty University
- Marymount University
- Norfolk State University
- Radford University
- Regent University
- University of Virginia

CAE-2Y

- Danville Community College
- Lord Fairfax Community College
- Northern Virginia Community College
- Thomas Nelson Community College
- Tidewater Community College

CAE-R

- George Mason University
- Virginia Tech

CAE National Resource Center

- Northern Virginia Community College

CAE-CO

- Virginia Tech

CCI STRATEGIC FRAMEWORK

4

The CCI has two primary objectives: to build world-leading research and innovation capabilities and to help close the workforce gap in cybersecurity in the Commonwealth. As a natural result of these efforts, CCI will power an engine of economic growth and diversity in cybersecurity in Virginia.

To do this, the CCI will develop a Network of information, services, and leadership that connects Regional Nodes led by public institutions of higher education to each other and to a major, world-class center of innovation capability in Northern Virginia, led by Virginia Tech.

The strategies and initiatives to meet the two principal CCI objectives follow. Within each objective are four strategies. Those strategies can be executed through initiatives that foster the CCI Network, build a central research capability, or strengthen Regional Nodes.

Throughout this strategic framework, examples of programs pioneered across the Commonwealth that can be replicated, amplified, connected, or leveraged to support CCI are highlighted.

Not all initiatives described here can be supported through the CCI appropriations in the Biennium budget. Indeed, most initiatives will fail without ongoing sustaining funds.

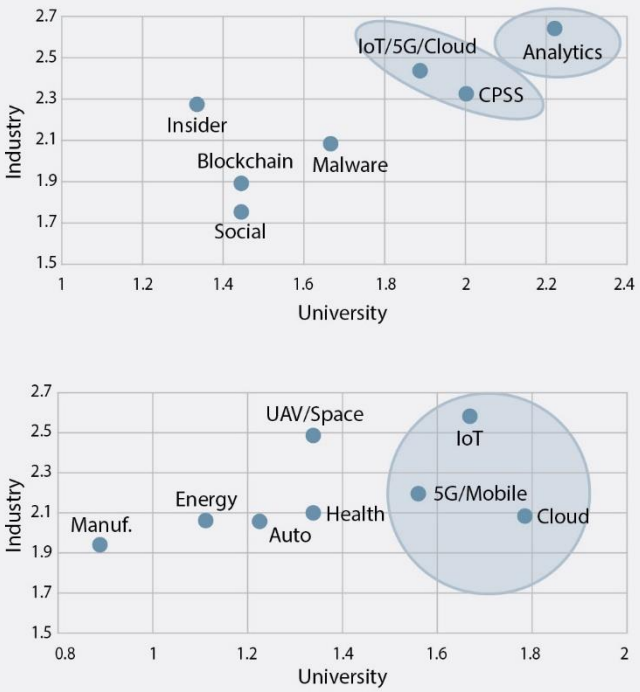
VISION: build an ecosystem of cyber-related research, education, and engagement that positions the Commonwealth as a world leader of cybersecurity.

MISSION: serve as an engine for research, innovation, and commercialization of next-generation cybersecurity technologies, and address the Commonwealth's need for growth of advanced and professional degrees within the cyber workforce.

CCI STRATEGIC FRAMEWORK 4

GOAL 1: BUILD WORLD-LEADING RESEARCH AND INNOVATION CAPABILITIES

The IT landscape is constantly changing, and cybersecurity approaches and technology must move faster. As new computing platforms, devices, and applications are developed—from cloud computing to 5G communications to autonomous systems—the cybersecurity challenges evolve. Putting the nation's most innovative minds to task to stay one-step-ahead of the cyber challenges of tomorrow presents an opportunity for increasing the economic growth of the Commonwealth.



Industry interest (vertical axis) and self-assessment of university capability (horizontal axis), on a scale from zero to three (three being high). There is high alignment between these indicators for IoT, 5G, CPSS, data analytics, and cloud computing, all of which are in CCI's focus on the intersection of security, data, and autonomy. Data is the result of a survey of CCI industry and university partners conducted by the Research and Technology Commercialization Working Group.

A survey of institutions of higher education in Virginia, along with more than 20 industry partners, found an opportunity in aligned industry interest and existing university capability in IoT, 5G communications, CPSS, data analytics, machine learning, and AI. CCI aims to target this opportunity space.

The last decade of the social-mobile Internet is giving way to the next decade of the IoT and the core technologies that will enable it such as 5G wireless. We seek to ensure that as these new technologies are developed, standardized, and deployed, they have the needed security features to ensure that the next generation of the Internet and the ecosystems built on top of it are underpinned with systematic security and privacy safeguards.

In each epoch of the Internet, security has been bolted on after new technologies experience major breaches, leading to patchy and poorly integrated security solutions. As we entrust our automobiles, factories, pacemakers, and energy distribution to the IoT, security must not be an afterthought.

Major IoT technologies are emerging, and 5G wireless standards are just now taking shape. This is an ideal time to systematically integrate security into edge computing, network slicing, and the protocols and frameworks that will enable smart infrastructure. CCI will leverage a consortium of selected industry partners to build standards, ecosystems, prototypes, and testbeds and be recognized as a global leader in CPSS.

Industry does not want to compete on security, and recognizes the need to collectively invest in ensuring that robust, interoperable solutions are widely available and systematically deployed. The economic success of IoT hinges on social trust in its security and privacy.

CCI STRATEGIC FRAMEWORK

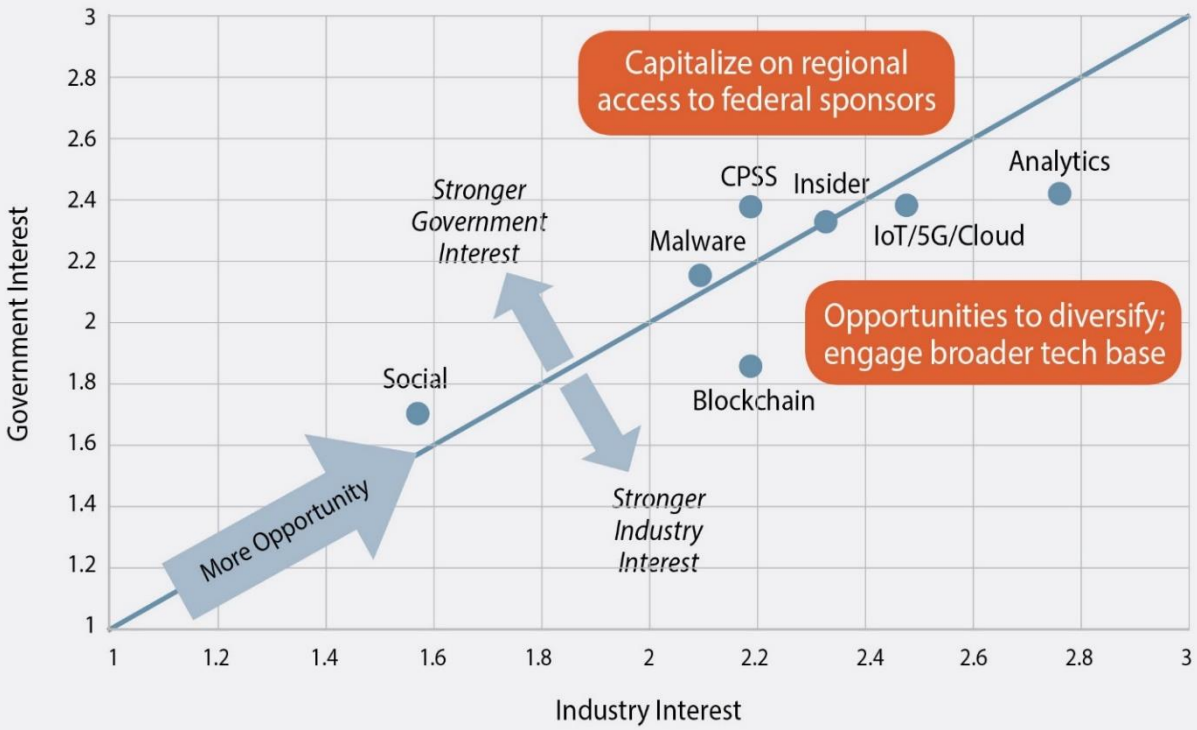
4

The current AI renaissance, driven by breakthroughs in machine learning (ML), promises to automate and make more efficient our homes, transportation networks, industrial processes, and national security. As safety-critical decisions are handed over to AI, users need confidence in the underlying ML to ensure its decisions are testable, repeatable, and auditable. We need to understand failure modes and be able to mitigate them.

Research into deep learning is creating systems that rival human-level performance on a wide range of tasks, but for the most part deep learning is a black box. It works better than past AI constructs, but when it makes mistakes, we often cannot explain them nor find ways to correct them. This is problematic when a self-driving car makes an unexplainable unsafe driving decision. It also opens up a new frontier for hackers who target AI algorithms to cause unexpected behavior, rather than more traditional computer systems, networks, and data.

CCI envisions building a world-leading multi-university team of researchers focused on this topic. It will explore topics such as explainable AI, test and evaluation of AI, and adversarial exploitation of AI and countermeasures. Research will include exploring both random faults and bounds on the impact adversarial elements can have on ML systems.

The U.S. national security apparatus is investing heavily in this topic. The Intelligence Community's Augmenting Intelligence using Machines program includes AI assurance as a core research thrust. The Pentagon's Joint AI Center combined with major new DARPA programs are focusing on this topic for military systems. Together, these three initiatives represent $6 billion in R&D investment in AI and ML over the next five years.



Government interest (vertical axis) and industry interest (horizontal axis) in cybersecurity technology areas on a scale from zero to three. IoT/5G/Cloud and data analytics have high interest from both industry and government, indicating high promise for research partnerships. Data is the result of a survey of CCI industry and university partners conducted by the Research and Technology Commercialization Working Group.

CCI STRATEGIC FRAMEWORK 4

STRATEGY 1.1: ESTABLISH CRITICAL MASS OF NATIONALLY RECOGNIZED RESEARCHERS

Studies show that density of companies, researchers, and VC in a single place is critical to building an ecosystem of entrepreneurship and economic growth in a given industry. Northern Virginia is a natural location for a CPSS cluster—it has the existing industry base and VC activity—but requires further research growth to spark innovation that diversifies the economy.

A co-working site will provide shared office space for students, professors, startups, and faculty, and will serve as a venue for hosting innovation programs. Adjacent office suites will support more established startups, venture capital firms, and innovation beachheads for large companies. This ecosystem seeks to provide the connective tissue that will accelerate the growth of organic relationships and partnerships across the ecosystem.

Initiatives include:

- Seek industry partners to guide, leverage, and support research projects across the Network.
- Recruit research-active faculty (led by senior or mid-career faculty) to build central competence in CPSS, with particular expertise in AI/ML and next-generation wireless.
- Incubate Hub at Virginia Tech Research Center – Arlington (VTRC-A) with space for faculty (VT and other institutions, as desired), industry, and spin-out incubation space. Identify permanent location, according to programmatic needs and partners.
- Recruit faculty aligned with CCI research focus and who will collaborate with researchers across network.

LEADING 5G SECURITY AS AN ENABLER FOR IOT

The emergence of 5G technologies could unlock many applications of IoT. Low latency in communications are necessary for high-speed, critical applications like autonomous vehicles. The ability to manage heterogeneous networks through tools like network slicing and flexible functions and capabilities will allow applications with a mix of existing and new components.

Securing the IoT infrastructure involves a combination of securing the edge devices, the communications networks, and the core computing in the cloud that provides services. Many embedded, real-time operating systems have no built-in security, which can make operational security difficult. Research in this area needs to develop lightweight security building blocks for embedded systems, work to focus new 5G standards and technologies in ways that help create a more secure ecosystem, and design new network defenses as the last vestiges of network perimeters literally disappear into “the fog.”

One of the first focus areas for CCI research and technology development programs will be in the intersection of cybersecurity with 5G networks for IoT applications.

STRATEGY 1.2: BUILD INDUSTRY AND GOVERNMENT PARTNERSHIPS TO FOCUS, SCALE, AND SUSTAIN RESEARCH

Through the unique combination of a Hub of world-leading CPSS research and innovation capacity and a robust and collaborative Network of research across the Commonwealth, CCI will be able to attract substantial investment from industry and government sponsors alike. CCI will use the state's investment in CCI to catalyze larger partnerships that will raise Virginia's stature as a premier location for talent and investment.

Initiatives include:

- Capture and execute programs that leverage expertise across the Network.
- Build IoT Security Research Alliance, establishing flagship partnerships across CPSS core focus areas.
- Seek opportunities to collaborate with federal partners on existing—or capture new—national research centers.
- Inventory and coordinate research capabilities across the Network to support industry and government partnerships.
- Identify and execute projects that leverage CCI expertise.

IOT SECURITY RESEARCH ALLIANCE

Given the alignment of academic and industry innovation strengths and growth opportunities in CPSS, CCI will build an IoT Security Research Alliance (ISRA) that brings together flagship partnerships with selected companies working across adjacent sectors of the IoT ecosystem. ISRA will be a multi-year initiative based around a defined set of projects and tasks, and an intellectual property model that will be familiar to the mobile industry.

The programs would include developing proof-of-concept systems to help debug and influence standards and provide common testing environments, open-source hardware and software projects that can be leveraged globally, and technology-focused engagement with regulators and policy makers in Washington, DC.

CCI envisions five to eight flagship partners within ISRA, aligned across the core focus areas of energy, transportation, and telecommunications. Partnerships anticipate engaging companies across the supply chain spectrum, including enabling technology vendors; integrators and original equipment manufacturers; and utilities and system operators.

Another key aspect of ISRA is the desire for partner companies to collocate within the CCI Hub or Regional Nodes, if advantageous to support research collaborations, either on a periodic sprint basis, or in a sustained capacity. Industry partners working shoulder-to-shoulder with researchers and innovators will help foster organic partnerships that will catalyze opportunity for everyone involved.

CCI STRATEGIC FRAMEWORK 4

CYBER EXCELLENCE ACROSS VIRGINIA

There are numerous resources across Virginia's institutions of higher education that can be brought to bear on CPSS research. Some highlights include:

George Mason University

- Center for Secure Information Systems
- DHS Center for Criminal Investigations and Network Analysis
- Center for Hardware and Embedded System Security and Trust
- Center for Assurance Research and Engineering
- Center for Cybersecurity Analytics and Automation
- Center of Excellence for Command, Control, Communications, Computing, Intelligence & Cyber
- Cryptographic Engineering Lab
- Computer Vision and Neural Networks Lab
- International Cyber Center
- Communications and Networking Lab
- Digital Forensics and Data Analytics Research Group
- Terrorism, Transnational Crime and Corruption Center
- Michael V. Hayden Center for Intelligence, Policy and International Security
- Center for Geospatial Intelligence
- Institute for Digital Innovation

James Madison University

- CyberDefense Lab X-Labs
- Center for Forensics and Information Security

Marymount University

- Cyber Center

Norfolk State University

- Center of Excellence in Cyber Security
- Information Assurance Research and Education Development Institute

Old Dominion University

- Center for Cybersecurity Education and Research
- Virginia Modeling, Analysis & Simulation Center
- Center for Innovative Transportation Solutions
- Consortium in Cyber Resilient Energy Delivery Systems
- Critical Infrastructure Resilience Institute
- Cybersecurity, Communications, and Networking Innovation (CCNI) Lab
- Emergent Risk Initiative
- Integrated Wireless Information Network Lab
- Strome Entrepreneurial Center
- Vision Lab

Radford University

- IMPACT (Innovative Mobile Personalized Accelerated Competency Training)
- Center for Information Security

University of Virginia

- LinkLab
- Cyber Innovation and Society
- National Security Policy Center
- Center for Business Analytics
- Center for the Management of Information Technology
- Center for Transportation Studies
- Data Science Institute
- Biocomplexity Initiative
- Center for Research in Intelligent Storage and Processing in Memory

Virginia Commonwealth University

- VCU Cyber Security Laboratory
- VCU Center for Analytics and Smart Technologies

Virginia Tech

- Center for Embedded Systems for Critical Applications
- Complex Networks and Security Research Lab
- Hume Center for National Security and Technology
- Information Technology Security Lab
- Security and Software Engineering Research Center
- Wireless @ Virginia Tech
- Virginia Tech Transportation Institute
- Discovery Analytics Center
- Virginia Tech Applied Research Corporation

STRATEGY 1.3: ESTABLISH A COMMONWEALTH-WIDE PLATFORM FOR CPSS RESEARCH

Virginia has many research capabilities to bring to bear—including the ODU Center for Cybersecurity Education and Research, the NSU Center of Excellence in Cyber Security, the VCU Cyber Security Laboratory, and the JMU Center for Forensics in Cyber Security. Virginia's universities also excel in the legal, social, and policy dimensions of CPSS. In addition, Virginia institutions enjoy partnerships with industry in their regions, which have emerging security challenges related to increased automation and connectivity. To make Virginia a national leader in cybersecurity, CCI will connect those assets to each other and the Hub.

Initiatives include:

- Establish an inventory of capabilities to facilitate partnerships among universities and with industry.
- Network and showcase innovations in annual workshops.
- Build on university strengths through recruitment of tenure-line and research faculty, and provide seed funds to catalyze promising research.
- Recruit companies to establish research centers near the Hub and Regional Node sites.

STRATEGY 1.4: DEVELOP AN ECOSYSTEM OF CPSS RESEARCH, EDUCATION, AND ENTREPRENEURSHIP

The natural byproduct of investment in research, innovation, degree programs, experiential education, and entrepreneurship is economic growth. However, Virginia cannot rely on the natural byproduct alone. Since spin-outs and startups are a driving force of high-growth economies, CCI will actively support CPSS-related entrepreneurship. CCI will not duplicate but leverage the broad array of established and emerging programs and structures that seek to build innovative capacity across the Commonwealth.

Initiatives include:

- Inventory and connect with existing innovation ecosystem programs across the Commonwealth.
- Host entrepreneurs-in-residence at the Hub to advise and support startups.
- Provide proof-of-concept grants to de-risk promising CPSS technologies.
- Connect regional cybersecurity research to economic development programs and leverage other Commonwealth investments such as those made by GO Virginia.

MACH37

MACH37 is designed to facilitate the creation of the next generation of cybersecurity product companies. MACH37's unique program design places heavy emphasis on the validation of product ideas and the development of relationships that produce an initial customer base and investment capital.

MACH37 is located at the Center for Innovative Technology. The Accelerator is operated by the MACH37 partners.

Upon acceptance into the program, participants will be coached in all aspects of identifying and building a sustainable business model. Upon completion of the MACH37 program, graduates will receive ongoing access to the MACH37 Stars Mentors Network throughout the life of their company.

CCI STRATEGIC FRAMEWORK 4

GOAL 1 SUMMARY: BUILD WORLD-LEADING RESEARCH AND INNOVATION CAPABILITIES

Strategy 1.1: Establish critical mass of nationally recognized CPSS researchers	▪ Seek industry partners to guide, leverage, and support research projects across the Network. ▪ Recruit research-active faculty (led by senior or mid-career faculty) to build central competence in CPSS, with particular expertise in AI/ML and next-generation wireless. ▪ Incubate Hub at Virginia Tech Research Center – Arlington (VTRC-A) with space for faculty (VT and other institutions, as desired), industry, and spin-out incubation space. Identify permanent location, according to programmatic needs and partners. ▪ Recruit faculty aligned with CCI research focus and who will collaborate with researchers across network
Strategy 1.2: Build industry and government partnerships to focus, scale, and sustain research	▪ Capture and execute programs that leverage expertise across the Network. ▪ Build IoT Security Research Alliance, establishing flagship partnerships across CPSS core focus areas. ▪ Seek opportunities to collaborate with federal partners on existing—or capture new—national research centers. ▪ Inventory and coordinate research capabilities across the Network to support industry and government partnerships. ▪ Identify and execute projects that leverage CCI expertise.
Strategy 1.3: Establish a Commonwealth-wide platform for CPSS research	▪ Establish an inventory of capabilities to facilitate partnerships among universities and with industry. ▪ Network and showcase innovations in annual workshops. ▪ Build on university strengths through recruitment of tenure-line and research faculty, and provide seed funds to catalyze promising research. ▪ Recruit companies to establish research centers near the Hub and Regional Node sites.
Strategy 1.4: Develop an ecosystem of CPSS research, education, and entrepreneurship	▪ Inventory and connect with existing innovation ecosystem programs across the Commonwealth. ▪ Host entrepreneurs-in-residence at the Hub to advise and support startups. ▪ Provide proof-of-concept grants to de-risk promising CPSS technologies. ▪ Connect regional cybersecurity research to economic development programs and leverage other Commonwealth investments such as those made by GO Virginia.

CCI STRATEGIC FRAMEWORK 4

GOAL 2: HELP CLOSE THE COMMONWEALTH'S WORKFORCE GAP IN CYBERSECURITY

While the precise size and scope of the gap between the demand for talent and the available workers in cybersecurity is difficult to determine, it is clear that it is large and growing, presenting a major challenge for current employers across the Commonwealth. Estimates based on cybersecurity job postings indicate that employers seek more than 33,000 workers in Virginia and 43,000 in the National Capital Region. Nationally, the workforce gap is estimated to exceed 300,000 jobs.

HRCyber

The Hampton Roads Cybersecurity Education, Workforce and Economic Development Alliance (HRCyber) is a partnership between educational institutions, government agencies, non-profit organizations, and private employers focused on developing educational pathways from high school through community college to four-year institutions and continued professional development providing a capable and fully trained cybersecurity workforce. To date, successful outputs from HRCyber's efforts include:

- Completion of a Cyber Counselor Workshop for high school career coaches and guidance counselors.
- Completion of two Cyber Saturday workshops for high school students and parents interested in learning more about cybersecurity education and career potential.
- Expansion of the ODU Cybersecurity virtual laboratory for training regional high school and college students.
- Completion of three articulation agreements making it easier for students to move between higher education institutions in the region (TCC&ODU, TNCC&ODU, NOVA&ODU).

Estimation of workforce gaps can be expected to vary depending on how "cybersecurity" is defined. Using a working definition that focuses on subject areas at the intersection of data, security and autonomy, a range of high-value employee skill sets can be identified, such as cryptography, compliance with legal standards, information security, computer network defense and forensics. A task force of major employers of the digital technology workforce, recently convened by GWP and supported by BHEF, is in the process of developing a list of generalist and specialist competencies that will provide more clarity concerning the specific workforce needs of industry. Competencies are currently being mapped to existing curricula in Virginia institutions of higher education to better align educational programs with industry needs.

To assess the need for expanding existing cybersecurity educational programs to meet the workforce requirements of the Commonwealth, the Educational Programs and Experiential Learning working group conducted a preliminary survey to determine the number of students currently enrolled in cybersecurity programs. In addition, contents of existing courses were reviewed.

Approximately 2,000 students are currently enrolled in cybersecurity-focused programs at public and private higher education institutions in the Commonwealth, and about 14,000 are enrolled in cybersecurity-related programs, including those in more generalized areas of computer and data sciences. Course content of cybersecurity-focused courses generally meets industry expectations, although it is anticipated that the curriculum mapping performed by the GWP task force and universities will further inform curricula updates.

CCI STRATEGIC FRAMEWORK 4

Assessments of the labor market further indicate the strong need for talent with real-world experiences. Just over 10 percent of the more than 30,000 job postings in Virginia related to cybersecurity are open to workers with less than three years of experience. Long-term internships, apprenticeships, and co-ops are critical. Additionally, experiential learning opportunities facilitate the process for applying for and receiving a security clearance prior to graduation.

While there are a number of educational programs in place across Virginia to address the types of cybersecurity talent needed, current programs are do not meet workforce capacity needs. Furthermore, most educational programs do not meet employee requirements related to cybersecurity certification and security clearance. Clearly, scaling existing cybersecurity education programs alone will not meet the large workforce gap. Additional approaches such as on-line learning enhanced by experiential learning and optimization of articulation agreements between community colleges and universities should be implemented.

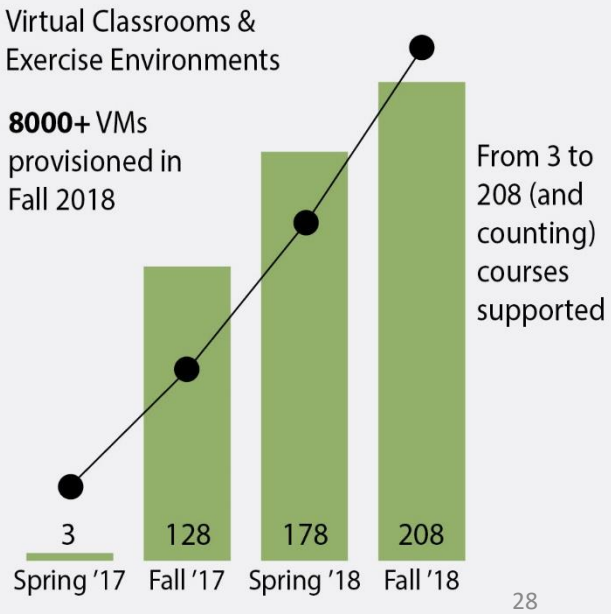
Pathways to the baccalaureate are essential for closing the workforce gap. Five community colleges have signed articulation agreements with ODU, GMU, and VT to enable students to move seamlessly from community college cybersecurity programs into baccalaureate programs.

Consideration must be given to assessing the pipeline of high school students interested in cybersecurity careers and, as necessary, promoting and facilitating the preparation of these students for enrollment in higher education programs. Virginia has already made a substantive and successful investment in this area by creating the Virginia Cyber Range. Initially funded by the Virginia General Assembly in 2016, this cloud-hosted virtual environment curates and hosts over 140 courseware materials accessible by schools and where students can practice their cybersecurity skills in immersive laboratory exercises. The Cyber Range currently supports 158 high schools, 16 community colleges and 13 universities in Virginia, involving over 1,600 student participants.

VIRGINIA CYBER RANGE

The Virginia Cyber Range is a Commonwealth of Virginia initiative with a mission to enhance cybersecurity education for students in the Commonwealth's public high schools, colleges, and universities. The Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Virginia Cyber Range provides an extensive Courseware Repository through virtual machines (VMs) for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students.

A primary feature of the Virginia Cyber Range is a cloud-hosted, virtual environment where students practice what they have learned in immersive, hands-on laboratory exercises to complement their cybersecurity courses.



CCI STRATEGIC FRAMEWORK 4

STRATEGY 2.1: CULTIVATE AND SUPPORT MEANINGFUL EXPERIENTIAL LEARNING OPPORTUNITIES

Students who participate in experiential learning programs are more prepared to enter the workforce and frequently have job offers before they graduate. Those experiences also help retain skilled workers in Virginia companies. The CCI Network provides a unique opportunity to bring together multiple stakeholders interested in offering paid internships to students and building robust academic credit-bearing standards into these experiences. In this way, students will be able to advance their learning without prolonging their time to graduation and while managing the cost of their education.

Several types of experiential learning are envisaged—full-time summer experiences lasting 10-14 weeks, part-time or full-time semester-long experiences in the fall or spring, year-long experiences that combine summer and school-year work, and capstone projects that bring real-world experiences into the classroom.

Initiatives include:

- Develop a portal of subsidized internship opportunities across Virginia, including a Co-Op 2.0 model.
- Build relationships with employers across the Commonwealth to develop experiential learning opportunities, including for credit-bearing, and provide matching funds for intern stipends.
- Promote undergraduate research experiences at participating institutions.
- Support experiential learning during the school year by providing opportunities for remote participation in classes, coordinating classes near company, and aligning with course credit.

CCI CO-OP 2.0 PORTAL

CCI envisions a "Co-Op 2.0" model that allows one or two full-time summer rotations off campus, but incorporates a part-time internship to ensure continuity during the academic year. Research suggests that experiential learning programs lasting a semester or more enhance future workplace engagement and wellbeing. Cooperative education ("co-op") is an experience that extends across multiple years, but frequently requires that the student spend several academic terms away from campus as a full-time intern, thus extending the time-to-degree by about a year. A 12–15 month commitment also allows an employer to commit to training (and security clearance sponsorship) that is required of a regular employee.

Given the importance of on-the-job experience to the cyber workforce in Virginia, experiential learning is critical to achieving the CCI vision. CCI should include matching funds for Co-Op 2.0 experiences.

The following models are consistent with a 12 month-minimum, 500 hour-minimum internship that allows regular academic progress (e.g., 30 or more earned credit hours per year) toward a degree, all of which will be coordinated through the CCI portal:

- internships at startups or established companies or organizations that are located near the student's campus;
- at an "Extension Office" on or adjacent to campus to employ interns during the academic year, allowing for a summer rotation to the employer site or a client site;
- at a Virginia employer site away from campus with internships designed into curricula that can be offered remotely through distance learning at the Hub or Regional Node;
- at the Hub, enabling a combination of the above models.

STRATEGY 2.2: ENHANCE THE PIPELINE OF STUDENTS ENTERING HIGHER EDUCATION PROGRAMS IN CYBERSECURITY AND RELATED FIELDS

The ability to scale and expand higher education cybersecurity training programs is highly dependent on the number of high school students interested in pursuing related careers. Emphasis will be placed on further development and propagation of existing programs addressing this need.

Dual enrollment pathways can increase the pipeline of students in cybersecurity and information assurance programs. These pathways should be mapped from certificates to associate degrees to baccalaureate degrees and should align with job requirements so that students have seamless transitions to the workforce or higher levels of education.

Examples of such programs include a pilot program funded by Virginia Tech involving a collaboration of high schools, community colleges, and a university in Southside Virginia. Established under the Virginia Provost's Initiative for Integrated Economic Development, the latter will build seamless pathways for students to transition from secondary education to the workforce via community colleges and a regional university offering undergraduate degrees. This will be accomplished via dual enrollment courses, longitudinal counseling across educational levels, professional development of in-service workers, and an ability to individualize programs of study. While this project was originally designed to promote graduation of K-12 teachers, the model is easily adaptable to enhancement of the cybersecurity student pipeline.

Also important are articulation partnerships that facilitate transfer of community college associate degree graduates to undergraduate programs. A number of such programs currently exist, including the successful ADVANCE partnership between George Mason University and Northern Virginia Community College (NOVA).

Initiatives include:

- Market cybersecurity careers and educational programs to middle, high school and college students, with special attention to increasing talent diversity.
- Establish a need-based scholarship program targeted to cybersecurity fields.
- Support further expansion of the Virginia Cyber Range courseware availability.
- Create and/or expand regional collaborations and articulation/transfer partnerships between secondary education, community college, university, and continuing education cybersecurity-related training programs.

ADVANCE

ADVANCE is a partnership between Northern Virginia Community College and George Mason University to streamline pathways from NOVA to Mason. Students benefit in multiple ways:

- Specialized, aligned curricula from NOVA to Mason ensure all credits transfer towards selected degree programs.
- Dedicated success coaches provide continuous support and guidance, from enrollment at NOVA to graduation from Mason.
- ADVANCE students are eligible for participation in recreational facilities, sporting and cultural events at NOVA and Mason.
- ADVANCE students are eligible to take select classes at Mason while enrolled at NOVA.

STRATEGY 2.3: ALIGN CURRICULA OF HIGHER EDUCATION PROGRAMS WITH CYBERSECURITY INDUSTRY NEEDS

Significant progress in aligning higher education curricula with industry needs is already being made by a task force convened by GWP and supported by BHEF. Generalist and specialist competencies are currently being mapped to existing curricula of multiple universities to better align educational programs with industry needs. Further refinement of competencies specifically supportive of or focused on cybersecurity will ensure that graduates are adequately prepared for employment. Consideration will be given to meeting the certification and security requirements of jobs in the field.

In addition, employers across Virginia and beyond require a workforce with rich analytical, communication, and creative problem solving skills. CCI should build on interdisciplinary approaches to cyber education already underway across Virginia. For example, William and Mary's Center for Legal and Court Technology has a writing competition dedicated to innovative legal issues likely to arise from AI, the IoT, and related technologies. ODU's academic programs in cybersecurity are intentionally interdisciplinary, including departments in Engineering, Sciences, Businesses, and Arts & Letters.

Initiatives include:

- Support the development of a shared understanding of whether educational programs meet industry certifications and standards for generalist and specialist skills.
- Work with federal agencies to provide streamlined pathways between higher education programs and jobs requiring security clearance.
- Engage federal agencies on experience and education required for jobs serving federal government.
- Study and track changes in labor market to support strategic investment.
- Revise and develop curricula and experiential educational programs in accordance with cybersecurity industry needs, certifications, and security clearance requirements, with an emphasis on interdisciplinary learning.

GREATER WASHINGTON PARTNERSHIP CYBER CREDENTIALING PROGRAM

The Greater Washington Partnership has created the Capital CoLAB, an alliance of university and business leaders. Among several projects the CoLAB will undertake is the creation of unique regionwide credentials to increase the quantity and quality of digital technology talent emerging from local undergraduate programs. Developed jointly by businesses and universities, the credentials will be recognized by regional businesses as differentiators in hiring and deploying talent. The Business Higher Education Forum is partnering with the Collaborative to develop student pathways to earn the credentials. The digital technology credentials are part of the Business Roundtable's new Workforce Partnership Initiative (WPI) to tackle current and future skills development challenges and drive economic growth in seven regions, including the Capital Region, around the United States.

STRATEGY 2.4: INCREASE THE NUMBER OF STUDENTS GRADUATING FROM HIGHER EDUCATION CYBERSECURITY PROGRAMS

A number of institutions are already growing their cybersecurity-related course and degree offerings to prepare their students for the modern workforce. There is an opportunity for CCI to align with and amplify these efforts. However, increasing the number of graduates through traditional means is a relatively expensive enterprise that alone cannot be expected to address the significant workforce needs. Therefore, in addition to scaling existing programs, other models of education will need to be developed. Examples include use of machine learning to customize and accelerate instruction, expansion of on-line learning and integration of experiential learning (internships, co-ops, etc.) to enrich and better prepare graduates.

CYBER EDUCATION PILOT

Given the scale of the existing workforce gap in cybersecurity-related fields in the Commonwealth (and across the nation), it is unlikely that the gap can be closed solely with traditional four-year degrees. The CCI should support pilot programs across the Commonwealth to create innovative approaches to education, which meet the following criteria:

- Rapidly scalable
- High quality
- Aligned with industry needs
- Not increase time-to-degree
- Not increase student loan burden
- Incorporate experiential learning

Many institutions of higher education have initiated programs that meet many of these criteria through dual enrollment, two-to-four-year programs, online learning, among others.

CCI should work with institutions across the Network to bundle degrees and certificates, both within one member institution and between institutions. For example, a coordinated 3+2 or 4+1 program that results in BS and MS degrees in five years could be more efficient for the student than pursuing each degree separately. Likewise, cyber degree pathways between Virginia's community colleges and four-year campuses that can be completed in four years should be prioritized. Certificate programs should be coordinated with BS, MS, and PhD programs so that certificates offered through one institution can be combined with degrees from another CCI member institution.

Initiatives include:

- Publish an inventory of degree, certificate, and course offerings at participating CCI institutions, and conduct ongoing assessments of programs.
- Coordinate degrees and certificates to provide packages that accelerate time to degree.
- Align CCI faculty recruitment with education focus of the Hub and Regional Nodes.
- Create a cyber education pilot grant program to fund innovative approaches to student training, and support faculty recruitment to execute pilots.
- Offer select professional certifications and courses.
- Commit half of 2018-2020 Biennium budget degree production in data science and technology to cybersecurity fields.
- Scale existing degree and certificate programs in alignment with cybersecurity needs assessments conducted by the Network.

GOAL 2 SUMMARY: HELP CLOSE THE WORKFORCE GAP IN CYBERSECURITY IN THE COMMONWEALTH

Strategy 2.1: Cultivate and support meaningful experiential learning opportunities	▪ Develop a portal of subsidized internship opportunities across VA, including a Co-Op 2.0 model. ▪ Build relationships with employers across VA to develop experiential learning opportunities, including for credit-bearing, and provide matching funds for intern stipends. ▪ Promote undergraduate research experiences at participating institutions. ▪ Support experiential learning during the school year by providing opportunities for remote participation in classes, coordinating classes near company, and aligning with course credit.
Strategy 2.2: Enhance the pipeline of students entering higher ed cybersecurity programs	▪ Market cybersecurity careers and educational programs to middle, high school and college students, with special attention to increasing talent diversity. ▪ Establish a need-based scholarship program targeted to cybersecurity-related fields. ▪ Support further expansion of the Virginia Cyber Range courseware availability. ▪ Create and/or expand regional collaborations and articulation/transfer partnerships between secondary education, community college, university, and continuing education cybersecurity-related training programs.
Strategy 2.3: Align curricula of higher ed programs with cybersecurity industry needs	▪ Support the development of a shared understanding of whether educational programs meet industry certifications and standards for generalist and specialist skills. ▪ Work with federal agencies to provide streamlined pathways between higher education programs and jobs requiring security clearance. ▪ Engage federal agencies on experience and education required for jobs serving federal government. ▪ Study and track changes in labor market to support strategic investment. ▪ Revise and develop curricula and experiential educational programs in accordance with cybersecurity industry needs, certifications and security clearance requirements, with an emphasis on interdisciplinary learning.
Strategy 2.4: Increase the number of students graduating from higher ed cybersecurity programs	▪ Publish an inventory of degree, certificate, and course offerings at participating CCI institutions, and conduct ongoing assessments of programs. ▪ Align CCI faculty recruitment with education focus of the Hub and Regional Nodes. ▪ Coordinate degrees and certificates to provide packages that accelerate time to degree. ▪ Create a cyber education pilot grant program to fund innovative approaches to student training, and support faculty recruitment to execute pilots. ▪ Offer select professional certifications and courses. ▪ Commit half of 2018-2020 Biennium budget degree production in data science and technology to cybersecurity fields. ▪ Scale existing degree and certificate programs in alignment with cybersecurity needs assessments conducted by the Network.

CCI IMPLEMENTATION 5

STRUCTURE

A summary of the two principal components of the CCI Network—the Hub and the Regional Nodes—appears below. The Hub serves as the coordinating mechanism for the CCI Network and provides a platform for collaboration and a portal to opportunities with industry and government.

The Hub will have a strong business development team to build new holistic partnership opportunities, academic specialists to support the alignment of curricula and establishment of transfer agreements, and dedicated data analysts to continuously assess the employment and technology landscape to support strategic decisionmaking.

As the focal point for the CPSS research and entrepreneurship activities for the Network, the Hub must attract talent and partners alike. By collocating leading faculty with an entrepreneur-in-residence, industry, and startups, the Hub will spur company creation and technology commercialization.

Finally, richly connected Nodes across the Commonwealth will be portals to research capabilities, local economies, and educational resources. By organizing around regional ecosystems and capabilities, CCI can be tailored and focused to have maximum impact across the diverse Virginia communities.

HUB		REGIONAL NODES
Management of Network aspects of CCI for whole state	Concentrated program of research and innovation leadership in CPSS	Regional ecosystems aligned with CCI goals
▪ Engage in business development to facilitate holistic partnerships on educational programs, internships and research across Network ▪ Facilitate showcases, networking, and working meetings to share, align, and normalize Network capabilities ▪ Run commercial innovation enhancement programs, including seed and proof-of-concept grants ▪ Lead development of standard policies, agreements, shared curricula resources ▪ Track metrics and economic landscape to support CCI reporting and planning ▪ Develop CCI annual report to VRIC ▪ Support development of Node plans ▪ Coordinate and host Leadership Council, Technical Advisory Board, and Expert Review Panels	▪ Hire faculty to build leading competence in CPSS, with particular expertise in AI/ML and next-gen wireless ▪ Provide space for hosting researchers from across Network on short- or long-term basis ▪ Provide co-working space for researchers, students, startups, and partners, as well as adjacent space for more established startups, venture capital firms, and beachheads for large companies ▪ Build partnerships with research and development capabilities at the Nodes ▪ Offer select professional certifications and courses	▪ Partner on research and innovation with the Hub and across the Network ▪ Build on research and workforce in region, aligned with regional attributes, industry, and capabilities ▪ Strengthen research programs in CPSS, with particular expertise in AI/ML and next-gen wireless ▪ Partner with innovation programs and facilities to support industry co-location ▪ Support development of innovative educational partnerships and programs to grow cyber workforce in region ▪ Facilitate student engagement in internships ▪ Grow degree production in cyber-related fields, and increases inclusion of cyber courses across all degrees

CCI IMPLEMENTATION 5

GOVERNANCE

Every component of CCI's governance structure should add value. We seek advice and guidance from stakeholders across the state, and from experts across the nation. We seek to be agile, with decisions made with the necessary speed. We seek to ensure that CCI actions align with a broader strategy.

VRIC

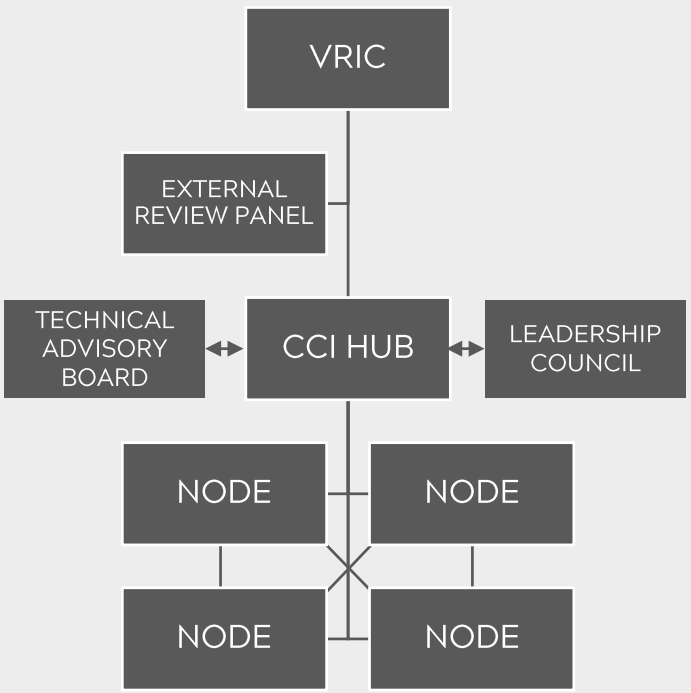
Source of funding for CCI programs, ensures accountability, and provides critical assessment and feedback for CCI

External Review Panel

Technical experts providing independent review of progress against goals annually, reports findings to VRIC

Technical Advisory Board

Leaders from industry and government providing advice and guidance on strategic direction of CCI



Leadership Council

Leaders of Nodes and Hub, chaired by CCI Executive Director

- Develops policy, develops and champions CCI budgets to the VRIC, Virginia General Assembly
- Advises on technical focus of research programs
- Advises on evolution and focus of educational programs (e.g., curricula/skills for investment and growth)
- Reviews metrics to ensure alignment with goals
- Creates roadmap for evolution of educational and research programs
- Pre-reviews Node plans to recommend to VRIC for certification

CCI Hub

- Leads development of standard agreements and shared resources
- Engages stakeholders to understand and influence requirements for cyber workers (e.g., educational attainment and work experience).
- Convenes expert panels to review proposals for faculty recruitment and seed grants from Nodes prior to releasing funds or forwarding to VRIC
- Houses data team to track metrics and economic landscape to support reporting and strategic planning
- Develops CCI annual report to VRIC; coordinates Leadership Council, Technical Advisory Board, and External Review Panel

CCI Regional Nodes

- Convenes institutions of higher education to support transfer and articulation agreements, alignment with CCI standards
- Facilitates regional institution engagement with CCI
- Lead acts as fiscal agent for regional institutions
- Aligns resources and programs with regional goals and deliverables.

CCI IMPLEMENTATION 5

REGIONAL NODE CERTIFICATION

The Virginia Research Investment Committee is responsible for certifying the Regional Nodes. CCI envisions between four and six Regional Nodes across the Commonwealth. Regional institutions should come together to develop a plan for CCI implementation in the region. The plan will be submitted to the VRIC by an institution of higher education. VRIC should consider forming a working group to establish next-steps for Node certification.

Certification should indicate commitment to the vision and program of CCI, the ability to implement the CCI program, and will serve as a common brand of quality in cyber education and research across the Network.

There are four categories of qualities required of a Node, shown below.

1 Commitment to cyber workforce development:

- 50 percent of 2018–2020 Biennium budget degree production in data science and technology dedicated to cyber
- Commitment to innovate and align curricula with industry-driven certifications and standards
- Commitment to enabling and incentivizing experiential learning opportunities

2 Commitment to CCI research priorities:

- Ability to contribute to CPSS research
- Plan to expand research capabilities in CPSS-enabling technologies or vertical application spaces

3 Commitment to regional ecosystems

- Plan to engage regional institutions (higher education, industry, non-profit, and government)
- Identification of Node director
- One Node per region

4 Commitment to CCI Network

- Commitment to share data and information with CCI Network and to participate in Network events
- Commitment to put faculty recruited with CCI funds in Hub or Regional Node for at least one month
- Commitment to standards of institutional IT security (e.g., participation in the Virginia Alliance for Secure Computing and Networking)

CCI IMPLEMENTATION 5

PROGRAMS IN BUDGET

The CCI Network will have a variety of programs, summarized below, to implement its strategy. None of these programs can be self-sustaining indefinitely. Those that can be partially supported for two years by the Biennium budget appropriation for CCI are underlined.

Network Programs

Network Portal – one of the first tasks will be to generate a Network portal: a one-stop shop for cyber-related educational and research programs across the Network. This inventory of programs and capabilities will serve stakeholders in industry, government, and across the Network as they seek to partner, align, or invest in CCI.

Entrepreneurship Programs – the Hub will host and administer a portfolio of programs aimed at promoting technology translation, commercialization, and entrepreneurship. This includes hosting entrepreneurial support services and cohorts and providing small proof-of-concept and seed grants to catalyze larger research programs or technology commercialization. About $2 million per year is recommended for the seed grant and proof-of-concept fund.

Market Research – CCI must be responsive to the economic landscape and accountable to Virginia taxpayers. The Hub will house a small team to assess the labor market to support strategic decisionmaking, and track and report on CCI's programmatic performance.

Curriculum Alignment and Normalization – a valuable component of CCI will be to normalize cyber-related curricula and degrees across the Network to enable transfers between institutions, and to align those curricula with industry needs. This will happen regionally within Nodes, as well as Network-wide.

Holistic Industry Partnership Development– the CCI Hub will have dedicated business development personnel to enable the development of research partnerships, experiential learning opportunities, and talent development with industry partners across the Network.

Workshops and Showcases – in order to promote collaborations across the Network and beyond, and partnerships with industry and federal sponsors, the Hub will host workshops and showcases of CCI outcomes.

Faculty Recruitment and Support

Research-Active Faculty Support – faculty at the Hub will be principally research faculty, with a primary mission of performing innovative research, development, and commercialization activities, with particular focus on next-generation communications technologies and AI/ML Faculty at the Hub will also training undergraduate and graduate students and post docs. After an initial start-up period, research faculty are expected to support most of their own 12-month salary through extramurally sponsored research programs.

Faculty Recruitment – providing funds for start-up packages to recruit and retain faculty scholars at the Hub and Nodes is one of the biggest opportunities to raise the stature of Virginia institutions. To promote collaboration across the Network, faculty recruited with these funds should align with the goals of the Network.

Faculty Support – faculty at the Nodes will enable both the research and workforce objectives of CCI. Faculty support will enable research and educational program growth in cyber programs across the Network.

Internships

Co-Op 2.0 Intern Stipends – experiential learning is critical to the success of CCI. It provides the real-world experience that employers demand and establishes a sticky pipeline of employees for Virginia firms. A stipend of up to $10 thousand per student per year—matched by the industry partner or research grant—should be administered through the Hub. A budget of up to $5 million per year—supporting 500-830 students (current degree production in cyber-focused fields)—is recommended.

CCI IMPLEMENTATION 5

BUDGET SUMMARY

	INCLUDED IN BIENNIUM BUDGET			ADDITIONAL FUNDS	
	Capital (in first year)	Hub (in second year)	Scaling and Faculty Recruiting (in second year)	Additional Funds to Scale	Base Funds at Scale (annual)
Hub	$3M - $1M in equipment, renovation, and furniture for temporary location - $2M towards permanent facility	$9.4M - $4.5M startup funds for research-active faculty - $3M for Network programs - $0.75M in rent - $1.15M in operational support	*Can apply*‡	$14M - $9M startup funds for research-active faculty - $5M for equipment and permanent facility	$11.5M - $4M for research-active faculty support - $5M for Network programs - $1M for education pilot program‡ - $1M in rent - $1.5M in operational support
Nodes	$2M to upfit Nodes		*Can apply*‡	$26M - $20M for scaling and faculty recruitment†‡ - $6M to upfit Nodes	$11.5M - $10M for faculty support - $1.5M for Network programs
Internships		$0.6M for internship match (up to $10k per student per year for 60-100 students) ‡			$5M for internship match (up to $10k per student for 500-830 students) ‡
Total VA	**$5M**	**$10M**	**$10M**	**$40M**	**$28M annual**
Leverage		**$0.6M**	**$10M**	**$20M**	**$35M annual**
TOTAL	**$5M**	**$10.6M**	**$20M**	**$60M**	**$63M annual**

Leverage refers to funds that will scale Virginia's investments in the initiative. In the case of internship stipends, faculty recruiting, scaling, and education pilot, this is a 1:1 match with non-state funds. The match should not need to go through the CCI program to count (for example, stipends paid directly to interns are an appropriate match). In general, funds for faculty recruitment should be matched by the host institution through non-state funds.

For base funds, leverage also includes scaling through sponsored research. At scale, we anticipate annual research expenditures from CCI to be on the order of $30M. Leverage from economic growth not included in table; biennial economic development assessments are planned.

Additional funds for scaling are recommended to begin in the FY2020-2022 Biennium budget.

†Hub and Nodes can apply for faculty recruitment funds
‡Requires match

CCI IMPLEMENTATION

5

TIMING

The timing CCI implementation is shown below. The first phase, through 2019, will be focused on hiring core personnel for the Hub. It will also be spent certifying Regional Node leaders and beginning the process of funding faculty recruitment and capital improvements, as appropriate.

Through phase II, the Network will continue to grow, establishing new programs and relocating the Hub, as programs necessitate.

After the first four years, CCI will enter a period of sustained growth and evolution, adjusting with agility to an evolving technology landscape and workforce environment.

PHASE I

FY2019-2020

- Hire CCI Executive Director, director of research, business development and data teams
- Develop strategic plans and certify Regional Nodes
- Build CCI Network Portal
- Begin pursuing holistic business partnerships
- Host research roadmap workshop
- Establish Technical Advisory Board, Leadership Council, External Review Panel
- Rent and upfit space to incubate Hub in VTRC-A, explore opportunities for new space
- Hire 15 research, instructional, tenure-line faculty
- Launch IoT Security Research Alliance
- Upfit Regional Nodes, as necessary
- Develop and submit applications to recruit faculty and scale initiative at Hub and across Nodes
- Begin to normalize curricula within Nodes

PHASE II

FY2021-2022

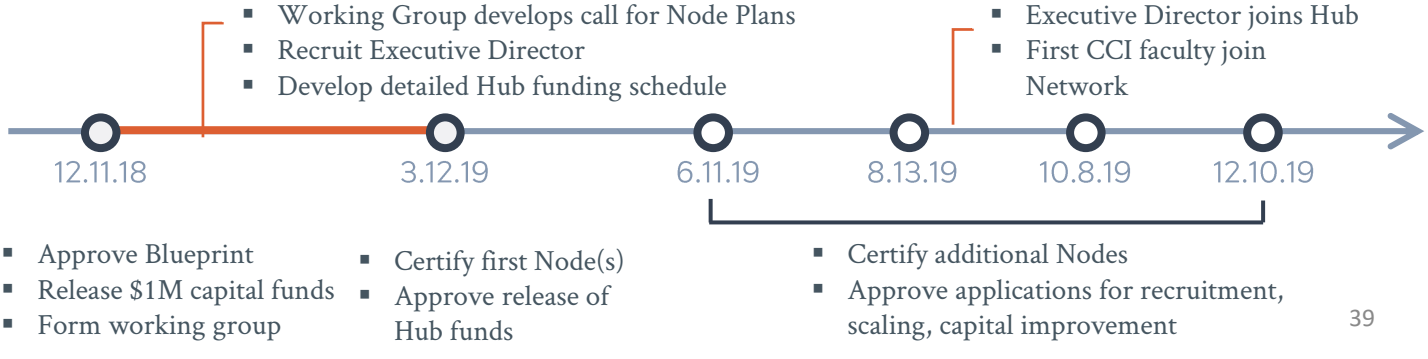
- Establish CCI advertising and marketing plan
- Internship portal begins, placing up to 300 interns
- Host showcases, annual CCI Network meetings
- Refine programs based on performance metrics and data
- Hire 25-30 research, instructional, tenure-line faculty
- Hire entrepreneur in residence
- Hub moves into new space
- First education pilot program(s)
- Seed grants for research at Hub and across Nodes
- Host showcases, research roadmap workshop

PHASE III

FY2023+

- Grow internship programs based on market requirements
- Continue to refine educational and industry partnership programs based on metrics and data
- Align and normalize curricula across Network
- Win increasing levels of research funding, including national research center
- Continue to grow research capability across Network

YEAR ONE IMPLEMENTATION



CCI IMPLEMENTATION 5

CONTINUOUS IMPROVEMENT AND EVOLUTION

CCI seeks to be agile and accountable. The Initiative will include mechanisms to continually assess the technological, economic, and workforce landscape and adjust strategy and investments to have the largest impact.

Measurement and Knowledge Management

The CCI Hub will house a small team dedicated to collecting, analyzing, and disseminating key indicators for the CCI program and the environment in which it operates. This office will assess the labor market across the Commonwealth, and will coordinate with the Regional Nodes to assess market needs in their regions. The office will track scholarly production and technology commercialization performance against benchmarking peers. The office will commission biennial economic impact studies of CCI programs. In total, by providing accurate baseline data and tracking performance metrics, the office will support strategic decisionmaking and accountability to VRIC and other stakeholders.

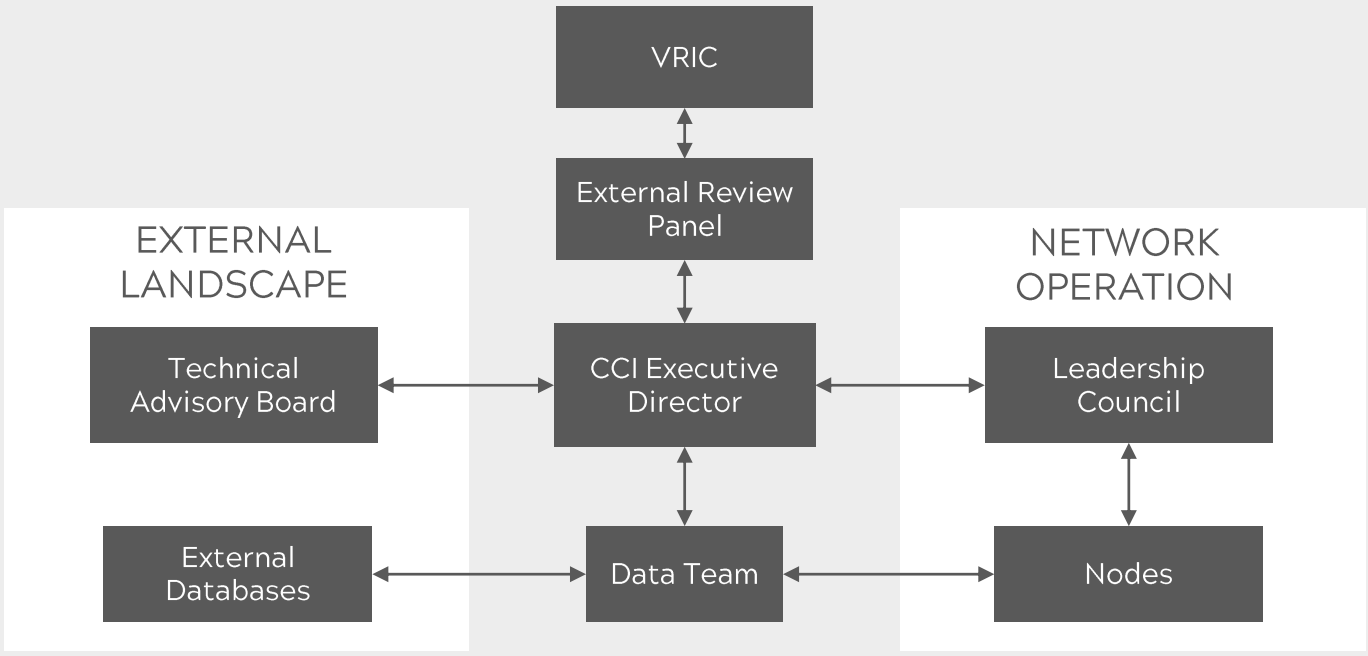
Annual Reporting

CCI will provide an annual report on CCI performance and achievements in research, commercialization, and talent development. It will be reviewed by the External Review Panel, who will report their findings to VRIC.

Regional Nodes will create multi-year plans to build CPSS translational research capacity, unique to the strengths of the relevant Node. Updated annually, these plans will describe how efforts will contribute to CCI goals.

External Advice and Guidance

CCI will seek guidance and advice from key stakeholders within the Commonwealth, as well as from national and international technical experts. The CCI Hub will convene a Technical Advisory Board to provide strategic feedback and guidance for the CCI program. The Hub will also convene panels of experts to review and assess proposals for funding—including seed grants and proof-of-concept funds—through the Network.



CCI IMPLEMENTATION 5

METRICS

CCI metrics must align with the stated goals of the appropriations: closing the workforce gap in cybersecurity, national leadership in CPSS research, and a robust ecosystem of entrepreneurship and technology commercialization.

CCI will measure its success using a robust, diverse set of well-established metrics. We will seek to measure not just what is easy to count, but what is meaningful. That will require intentional data collection and assessment by dedicated teams—these data are not universally measured.

It may take time to establish baseline counts and associated targets for many of these measures. Developing the baseline and targets will be one of the first tasks of the CCI Hub.

Relevant metrics may evolve over time as the CCI gains maturity. Implementing a new program now will not lead to new graduates in six months. Therefore, we will seek to implement new measures as time goes on.

Metrics will be reported at meetings of the CCI Leadership Council, and progress against them will be communicated in CCI annual reports.

	INPUT YEARS 1+	OUTPUT YEARS 3+	OUTCOME YEARS 5+
RESEARCH	▪ Faculty hired across at Hub and across Nodes (number of junior, mid-career, and senior) ▪ Submitted/awarded grants and contracts	▪ Research expenditures at Hub and across Nodes (number and size of grants awarded) ▪ Scholarly output (publication number and quality) ▪ Scholarly output with collaboration across Network ▪ Innovation output (patents and licenses)	▪ Leadership of national centers ▪ Faculty fellowships and awards in national professional societies
COMMERCIAL -IZATION	▪ Student and faculty participation in entrepreneurship programs	▪ Companies launched (both university spinout and overall) ▪ Industry partners collaborating on or funding research	▪ VC investment (both university spinout and overall) in Virginia ▪ Companies with a presence in the Hub and at shared innovation facilities at Nodes
WORKFORCE	▪ Enrollment in cyber-focused degrees ▪ Enrollment in cyber courses as part of other degrees	▪ Degree production across all levels of education (associates, bachelor's, masters, PhDs) ▪ Internship/experiential learning participation	▪ Graduates working for Virginia employers after graduation ▪ Graduates work in the field after graduation ▪ Educational debt as ratio of starting salary

CCI IMPLEMENTATION 5

TARGETS

A critical early task for the CCI Network is to establish baselines for the metrics described previously. That will require establishing consensus across the Network about requirements for included degrees, courses, and curricula, defining appropriate categories for scholarship, and other dimensions. It will also require a thorough assessment of enrollment and degree production, research capabilities and expenditures, and innovation ecosystems. Finally, an assessment of the labor market landscape and benchmarking of similar programs across the country will support the development of targets.

To provide context for the ambitions of CCI, rough estimates of key metrics are provided below. Eight-year targets assume full support of base funds.

Note that general cyber-awareness among students across all degrees is a goal of CCI, not represented in the growth in cyber-focused degrees.

	Baseline	Δ FY2022	Δ FY2026
FACULTY PARTICIPATING ACROSS NETWORK	200	25	65
ANNUAL SCHOLARLY PUBLICATIONS ACROSS NETWORK	800	100	300
ANNUAL COMPETITIVE RESEARCH EXPENDITURES ACROSS NETWORK	(TBD)	$10 M	$30 M+
CUMULATIVE COMPANIES LAUNCHED	(TBD)	3	10
ANNUAL DEGREE PRODUCTION IN CYBER-FOCUSED DEGREES†	450	150	450

† Includes bachelor's and masters in cybersecurity, information security, and information assurance from Virginia public institutions of higher education; 2022 target includes 50 percent of Data Science and Technology degree production investments in Biennium budget; 2026 target includes may include growth from other sources. Private institutions of higher education in Virginia contribute an additional ~400 degrees per year in these fields.

CCI IMPLEMENTATION 5

GUIDELINES FOR CCI FACULTY RECRUITMENT

Eligibility

- Proposals can be submitted by a single institution or multiple institutions. Proposals from multiple institutions can be coordinated and submitted simultaneously. Independent colleges and universities based in Virginia may participate in proposals led by a public institution.
- Proposals can include a mix of start-up funds and endowment funds for CCI Eminent Scholars.
- The focus of the CCI Faculty Scholars program should be on recruiting talent from outside Virginia, but the program should be available to current rising star faculty subject to being recruited by another institution.
- Requests will be considered up to a maximum funding level (e.g., $2 million).
- Requests should come with a minimum 1:1 match from the institution(s) in non-state resources.

Proposal Content

- CCI Faculty Scholar to be recruited—the target(s)—should be named and a case should be made as to why the proposing institution(s) expects the target(s) to accept an offer.
- For CCI Faculty Scholars expected to contribute primarily to the research mission, preference should be given to those with a strong commercialization record.
- The proposing institution should describe how the Scholar will contribute to the research and/or teaching emphases of the Hub or Regional Node.

VRIC Review

- VRIC should vet the CVs of the target(s) with a panel that includes outside experts who can assess the potential of the target(s) to contribute at a world-class level to research, teaching, or commercialization.
- VRIC should consider proposals on a rolling basis.
- VRIC should provide a decision on a proposal within three months of proposal submission. If funding is denied, a brief summary of the reasons for the denial should be offered to the proposing institution.

Funding Process

- VRIC matching funds awarded for recruitment should be held in trust during the recruitment process for no longer than 12 months, after which the institution must reapply.
- An acceptance letter from the target should trigger release of funds.
- In the event that a CCI Faculty Scholar should leave the institution, the institution should, within 12 months of the separation of the CCI Faculty Scholar, provide a report on the remaining unencumbered VRIC funds, which should either be returned to VRIC or be included in a subsequent proposal to refill that position.
- Institutions receiving VRIC funds for CCI Faculty Scholars should provide a consolidated annual faculty activities report (one report for multiple awards) to both the CCI Hub and VRIC.

ACKNOWLEDGEMENTS

6

CCI benefitted from time, effort, and insights contributed by participants from dozens of institutions—public and private, higher education and industry—across the Commonwealth. Nearly 100 people gave their time and insights to the CCI over the course of four months. This includes members of the Advisory Council, members of each of four working groups, as well as a number of people who provided ad-hoc thoughts and advice throughout the process.

The drafters of the Blueprint would like to specially recognize the executive committee and the co-chairs of the working groups for their time and efforts.

CCI BLUEPRINT EXECUTIVE COMMITTEE

Sanju Bansal, Chief Executive Officer, Hunch Analytics
Rodney Blevins, Senior Vice President and Chief Information Officer, Dominion Energy
Charles Clancy, Executive Director, Hume Center for National Security, Virginia Tech
Deborah Crawford, Vice President for Research, George Mason University
James W. Dyke Jr., Member, Virginia Research Investment Committee; Member, GO Virginia; Senior Advisor, Virginia State Government Relations, McGuireWoods Consulting LLC
Eileen Ellsworth, President, Community Foundation for Northern Virginia
Tracy Gregorio, President, G2 Ops, Inc.
Bobbie Kilberg, President & Chief Executive Officer, Northern Virginia Technology Council
Theresa Mayer, Vice President for Research and Innovation, Virginia Tech (*chair*)
Michael Papay, Vice President and Chief Information Security Officer, Northrop Grumman
Brian K. Payne, Vice Provost for Academic Affairs, Old Dominion University
Scott Ralls, President, Northern Virginia Community College
Melur Ramasubramanian, Vice President for Research, University of Virginia
Sharon Simmons, Department Head, Computer Science, James Madison University
Erdem Topsakal, Chair, Department of Electrical and Computer Engineering, Virginia Commonwealth University
John Wood, Chairman and Chief Executive Officer, Telos

CCI BLUEPRINT WORKING GROUP CO-CHAIRS

Research and Technology Commercialization
Charles Clancy, Executive Director, Hume Center for National Security, Virginia Tech
Deborah Crawford, Vice President for Research, George Mason University

Educational Programs and Experiential Learning
Cyril Clarke, Interim Executive Vice President and Provost, Virginia Tech
Brian K. Payne, Vice Provost for Academic Affairs, Old Dominion University

Partnerships and Investment
Tracy Gregorio, President, G2 Ops, Inc.
Brandy Salmon, Associate Vice President for Innovation and Partnerships, Virginia Tech

Finance and Government Relations
Bobbie Kilberg, President & Chief Executive Officer, Northern Virginia Technology Council
Dwight Shelton, Vice President for Finance and Chief Financial Officer, Virginia Tech

ACKNOWLEDGEMENTS

6

CCI BLUEPRINT ADVISORY COUNCIL

Leigh Armistead, President, Peregrine Solutions
Shawn Avery, President and CEO, Opportunity Inc.
Sanju Bansal, Chief Executive Officer, Hunch Analytics
Greg Baroni, Chairman and Chief Executive Officer, Attain LLC
Paul Barrett, College of Business and Economics, Longwood University
Scott Bevins, Associate Provost for Information Services, UVA Wise
Peter Blake, Director, State Council of Higher Education for Virginia
Dan Bowden, Vice President and Chief Information Security Officer, Sentara Healthcare
Jamie Camp, Director of Grants and Partnerships, Richard Bland College
Todd Estes, Director, Career Education Programs & Workforce Partnerships, Virginia Community College System
Megan Healy, Chief Workforce Development Advisor to Governor Northam
Peter Hesse, Chief Security Officer, 10Pearls
Marthe Honts, Sponsored Programs Director, Virginia Military Institute
Rick Joyce, Department of Information Technology, Radford University
Robert M. Lewis, Chair, Department of Computer Science, College of William and Mary
Henry Light, Council Secretary, State Council of Higher Education for Virginia
Keith Mellinger, Dean, College of Arts and Sciences, University of Mary Washington
Michael Papay, Vice President and Chief Information Security Officer, Northrop Grumman
Toni Riedl, Chair, Department of Physics, Computer Science and Engineering, Christopher Newport University
Todd Rowley, Senior Vice President, United Bank
Lynn Seuffert, Associate for Research Investment, State Council of Higher Education for Virginia
Leo Simonovich, Vice President and Global Head, Industrial Cyber and Digital Security, Siemens Energy
Marianne H. Ward-Peradoza, Dean, School of Business and Technology, Marymount University
Dale Wesson, Vice President for Research and Economic Development, Virginia State University
Aurelia T. Williams, Director, Cybersecurity Complex, Norfolk State University

RESEARCH AND TECHNOLOGY COMMERCIALIZATION WORKING GROUP

Charles Clancy, Director, Hume Center for National Security, Virginia Tech (Co-Chair)
Deb Crawford, Vice President for Research, George Mason University (Co-Chair)
Simone Acha, Owner, Simone Acha Consulting
Chip Filer, Associate Vice President for Economic Development, Old Dominion University
Carl Elks, Department of Electrical and Computer Engineering, Virginia Commonwealth University
Todd Estes, Director, Career Education Programs & Workforce Partnerships, Virginia Community College System
Gabriel Galvin, Executive Director, The MITRE Corporation
Keith Holland, Assistant Head, Department of Engineering, Interim Vice Provost, James Madison University
Mitch Horowitz, Principal and Managing Director, TEConomy Partners LLC
George Hsieh, Director, Center of Excellence Cybersecurity Research, Norfolk State University
Steve McKnight, Vice President of the National Capital Region, Virginia Tech
Rob Merhige, Assistant Vice President for Commercialization and Compliance, University of Virginia
Mark Mykityshyn, Executive Chairman and CEO, Tangible Security
Michael Papay, Vice President and Chief Information Security Officer, Northrop Grumman
Ed Swallow, Senior Vice President of Civil Systems Group, The Aerospace Corporation
Thomas Weithman, President and Chief Investment Officer, MACH37; Managing Director and Vice President, Center for Innovative Technology

ACKNOWLEDGEMENTS

6

EDUCATIONAL PROGRAMS AND EXPERIENTIAL LEARNING WORKING GROUP

Cyril Clarke, Interim Executive Vice President and Provost, Virginia Tech (Co-Chair)
Brian Payne, Vice Provost for Academic Affairs, Old Dominion University (Co-Chair)
Sherif Abdelwahed, Department of Electrical and Computer Engineering, Virginia Commonwealth University
Scott Bevins, Associate Provost for Information Services, The University of Virginia's College at Wise
Isabel Cardenas-Navia, Director of Emerging Workforce Programs, Business Higher Education Forum
Liza Wilson Durant, Associate Dean, Strategic Initiatives and Community Engagement, George Mason University
Samy El-Tawab, Department of Integrated Science and Technology, James Madison University
Sandra Fourney, Engineering Director, Center of Excellence, Northrop Grumman Corporation
Jonathan Graham, Director, Information Assurance-Research Education and Development Institute, Norfolk State University
Chad Knights, Provost for Information and Engineering Technologies, Northern Virginia Community College
Christopher Kreider, Computer Science, Christopher Newport University
Henry Light, Council Secretary, State Council of Higher Education for Virginia
Keith Mellinger, Dean, College of Arts and Sciences, University of Mary Washington
Charles Reiss, Department of Computer Science, University of Virginia
Mary Sandy, Director, Virginia Space Grant Consortium
John Savage, Director, Cybersecurity Programs, Virginia Community College System
Jennifer Thornton, Director of Workforce Initiatives, Greater Washington Partnership

PARTNERSHIPS AND INVESTMENT WORKING GROUP

Tracy Gregorio, President, G2 Ops Inc. (Co-Chair)
Brandy Salmon, Associate Vice President for Innovation and Partnerships, Virginia Tech (Co-Chair)
Jenny Carter, Director, Workforce Partnerships, Virginia Community College System
Dean Evasius, Associate Vice President for Research Development, University of Virginia
Bill Hazel, Senior Advisor for Strategic Initiatives and Policy, George Mason University
Mary Ann Hoppa, Computer Science, Norfolk State University
Sharon Simmons, Head, Department of Computer Science, James Madison University
Eric Weisel, Director for Virginia Modeling, Analysis and Simulation Center, Old Dominion University
Chris Whyte, Wilder School of Government, Virginia Commonwealth University

FINANCE AND GOVERNMENT RELATIONS WORKING GROUP

Bobbie Kilberg, President and CEO, Northern Virginia Technology Council (Co-Chair)
Dwight Shelton, Vice President for Finance and Chief Financial Officer, Virginia Tech (Co-Chair)
Matt A. Conrad, Executive Director of Government and Board Relations, Virginia Commonwealth University
Betsey Daley, Associate Vice President for State Government Relations and Special Assistant to the President, University of Virginia
Ben Delp, Director of Research Development and Promotion, James Madison University
Ellen Davenport, Asst. Vice Chancellor, Governmental Relations, Virginia Community College System
Elizabeth Hooper, Director of State Government Relations, Virginia Tech
Paul Liberty, Vice President for Government and Community Relations, George Mason University
Annie Morris, Director of Government Relations, Old Dominion University
John Leonard, Executive Associate Dean, College of Engineering, Virginia Commonwealth University
Chris Whyte, Government Affairs Manager, University of Mary Washington
Aurelia T. Williams, Director, Cybersecurity Complex, Norfolk State University

ACKNOWLEDGEMENTS

6

INDUSTRY ROUNDTABLE (attendees on other working groups or advisory council not listed)

Ed Baine, Senior Vice President for Distribution, Dominion Energy (*sent comments*)
Simon Hartley, Vice President Business Development & Co-Founder, RunSafe Security
Carol Hawk, Acting Deputy Assistant Secretary, U.S. Department of Energy
Kevin Heaslip, Associate Director, Electronic Systems Lab, Hume Center, Virginia Tech
Dave Ihrie, Chief Technology Officer, Center for Innovative Technology
Michelle James, Vice President, Strategic Industry Programs, CTIA
Cathy McGhee, Director, Virginia Transportation Research Council, Virginia Department of Transportation
Dennis Manos, Vice President of Research, College of William and Mary
Jim Mollenkopf, Senior Director, Strategic Development, Qualcomm
Jonathan Porter, Chief Scientist, Federal Highway Administration, U.S. Department of Transportation
Christina Reilly, Senior Manager, Business Development, CTIA
Mark Sargent, Vice President of Certification, CTIA
Paul Schomburg, Director, Government & Public Affairs, Panasonic Corporation of North America
Mike Shulman, Program Manager, Automated Vehicles and CAMP, Ford (*sent comments*)
Katherine Wood, Head of Product, Global Cyber, Siemens USA
Reginald Viray, Virginia Tech Transportation Institute, Virginia Tech
Sam Visner, Director, National Cybersecurity Federally Funded Research and Development Center, MITRE

AD-HOC ADVICE

Diana Burley, Executive Director and Chair, Institute for Information Infrastructure Protection, George Washington University
Tom Dingus, Director, Virginia Tech Transportation Institute
Tim Hodge, Associate Vice President for Budget and Financial Planning, Virginia Tech
Rachel Holloway, Vice Provost for Undergraduate Academic Affairs, Virginia Tech
Diane Murphy, Chair, IT, Data Science, and Cybersecurity Department, Marymount University
Randy Marchany, University Information Technology Security Officer, Virginia Tech
Eric Paterson, Head, Kevin. T. Crofton Department of Aerospace and Ocean Engineering, Virginia Tech
David Raymond, Director, Virginia Cyber Range, Deputy Director, IT Security Lab, Virginia Tech
Jeff Reed, Willis G. Worcester Professor, Bradley Department of Electrical and Computing Engineering, Virginia Tech
Scott White, Director, Cybersecurity Program and Cyber Academy, George Washington University

OTHER SUPPORT

Kathy Acosta, Office of the Vice President for Research and Innovation, Virginia Tech
Christine Callsen, Hume Center for National Security and Technology, Virginia Tech
Karin Clark, LINK | The Center for Advancing Industry Partnerships, Virginia Tech
Melissa Elliot, Office of the President, Virginia Tech
Tracie Hase, Office of the Vice President, Northern Capital Region Operations, Virginia Tech
Shannon Harvey, Office of the Executive Vice President and Provost, Virginia Tech
Sarah Hayes, Virginia Tech
Laurel Miner, Chief of Staff, Office of the Vice President for Research and Innovation, Virginia Tech
Chris Yianilos, Executive Director of Government Relations, Virginia Tech
Lesley Yorke, Senior Director of Communications, Virginia Tech
Lisa Young, LINK | The Center for Advancing Industry Partnerships, Virginia Tech
Diane Zielinski, Office of the Vice President for Research and Innovation, Virginia Tech

APPENDICES

7

2018 Special Session I
Budget Bill - HB5002 (HB5002S1)
Bill Order » Office of Education » Item 252
Higher Education Research Initiative
Authority: Title 23.1, Chapter 31, Article 8, Code of Virginia

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.

2. The initiative shall consist of a primary Hub, located in Northern Virginia, and a network of Spokes across the Commonwealth with collaborating public institutions of higher education in Virginia and industry partners to build an ecosystem of cyber-related research, education, and engagement that positions the Commonwealth as a world leader of cybersecurity.

3. In collaboration with public institutions in the Commonwealth, Virginia Polytechnic Institute & State University shall serve as the anchoring institution and coordinate the activities of the Hub.

4. Out of this appropriation, $10,000,000 in the second year from the general fund is provided to the Virginia Research Investment Fund (VRIF) to scale the initiative and provide resources for faculty recruiting at both the Hub and Spoke sites. The VRIF will establish a process for public institutions of higher education in Virginia to seek certification as a Spokes site based on a plan for institutional investment, industry partnership, enrollment growth, and research focus areas. The Hub and certified Spokes sites will have the ability to seek matching funds for faculty recruitment and support for renovations and equipment. Certified institutions shall submit their funding request application to the Virginia Research Investment Committee established in § 23.1-3132 for review and evaluation. After completing its review, the Virginia Research Investment Committee, pursuant to § 23.1-3133, shall approve or deny the request for an allocation of funds.

5. Out of this appropriation, $10,000,000 in the second year from the general fund is provided for the leasing of space and establishment of the Hub by the anchoring institution and for the establishment of research faculty, entrepreneurship programs, student internships and educational programming, and operations of the Hub.

6. Out of the amounts authorized in Item C-52.10 of Chapter 836, 2017 Session, $5,000,000 in the first year shall be made available for renovations, space enhancements, and equipment.

2018 Special Session I
Budget Bill - HB5002 (HB5002S1)
Bill Order » Office of Education » Item 252
Higher Education Research Initiative
Authority: Title 23.1, Chapter 31, Article 8, Code of Virginia

(*continued*)

7. No later than December 1, 2018, Virginia Polytechnic Institute & State University shall provide to the Virginia Research Investment Committee (VRIC) a blueprint for the development and operation of the Commonwealth Cyber Initiative. This report will include such components as an outline of Virginia Tech's operating model of the Hub, a framework for Spoke sites and their interface with the Hub, an assessment of opportunities for industry partnerships and the commercialization of innovation, and a vision for both the short-term and long-term development of the initiative. The report will define the amount needed to establish the Hub including renovations, equipping and leasing of space, establishment of research faculty, entrepreneurship programs, student internships and educational programming, operations of the Hub, establishment of cyber-physical systems security at the Hub and at supporting Spoke sites across the Commonwealth, establishment of a machine learning lab at the Hub, and the amount for Virginia Research Investment Fund (VRIF) to scale the initiative and provide resources for faculty recruiting at both the Hub and Spoke sites. The report will clarify the process for public institutions of higher education in Virginia to seek certification as a Spoke site based on a plan for institutional investment, industry partnership, enrollment growth, and research focus areas. The Hub and certified Spoke sites will have the ability to seek matching funds for faculty recruitment and support for renovations and equipment. Certified institutions shall submit their funding request application to the Virginia Research Investment Committee established in § 23.1-3132 for review and evaluation. After completing its review, the Virginia Research Investment Committee, pursuant to § 23.1-3133, shall approve or deny the request for an allocation of funds.

APPENDICES

7

FACULTY AT VIRGINIA UNIVERSITIES WORKING IN CPSS

George Mason University

Alexander Levis
Anand Vidyashankar
Angelos Stavrou
Arun Sood
Avesta Sasan
Bijan Jabbari
Bill Roeting
Brian Mark
Cameron Nowzari
Carlotta Domeniconi
Constantinos Kolias
Daniel Barbara
Daniel Fleck
Daniel Menasce
Dorin Marcu
Dov Gordon
Duminda Wijesekera
Edward Huang
Elizabeth White
Emanuela Marasco
Fei Li
Foteini Baldimtsi
George Donahue
Gheorghe Tecuci
Hakan Aydın
Harry Wechsler
Hassan Gomaa
Hemant Purohit
Houman Homayoun
Jana Kosecka
Jeff Offutt
Jens-Peter Kaps
Jim Jones
John Shortle
Jon Bell
Jyh-Ming Lien
Kai Zeng
Kathy Laskey
Kris Gaj
Kun Sun
Lance Sherry
Mark Pullen
Massimiliano Albanese
Noseong Park
Ozlem Uzuner
Parth Pathak
Paul Amman
Paulo Costa
Rajesh Ganesan
Robert Simon
Sanjeev Setia
Sean Luke
Setarah Rafatirad
Shvetha Soundararajan
Song Min Kim
SongQing Chen
Sushil Jajodia
Thomas LaToza
Vadim Sokolov
Vivian Motti
Xiang Chen
Xinyuan Wang
Yup Cheng
Yutao Zhong
Zhi Tian
Zoran Duric

James Madison University

Florian Buchholz
Hossain Heydari
Michael Kirkpatrick
Mohamed Aboutabl
Xunhua Wang

Marymount University

Diane Murphy
Michelle Liu
Alex Mbaziira
Susan Conrad

Norfolk State University

Cheryl Hinds
George Hsieh
Jonathan Graham
Yen-Hung Hu

Old Dominion University

Adrian Gheorghe
C. Ariel Pinto
Chung-Hao Chen
Chunsheng Xin
Cong Wang
Dimitrie Popescu
Hongyi Wu
Jiang Li
Jingwei Huang
Khan Iftekharuddin
Lee Belfore
Masha Sosonkina
Michele Weigle
Oscar Gonzalez
Ravi Mukkamala
Sachin Shetty
Stephan Olariu
Weize Yu
Yiannis Papelis

APPENDICES

7

FACULTY AT VIRGINIA UNIVERSITIES WORKING IN CPSS

University of Virginia

Anil Vullikanti
Arsalan Heydarian
Ashish Venkat
Barry Horowitz
Ben Calhoun
Brad Campbell
Brian Park
Brian Smith
Cody Fleming
Dan Quinn
David Evans
David Wu
Devin Harris
Don Brown
Donna Chen
Haiying Shen
Homa Alemzadeh
Jack Davidson
Jack Stankovic
James Lambert
John Lach
Kamin Whitehouse
Kevin Sullivan
Laura Barnes
Lu Feng
Madhur Behl
Maite Brandt-Pearce
Malathi Veerarghavan
Marty Humphrey
Mary Lou Soffa
Matt Gerber
N. Rich Nguyen
Nicola Bezzo
Peter Beling
Ronald Williams
Steve Bowers
Yacov Haimes
Yonghwi Kwon
Yuan Tian

Virginia Commonwealth University

Carl Elks
Eyuphan Bulut
Irfan Ahmed
Milos Manic
Sherif Abdelwahed
Tamer Nadeem
Thang Dinh
Yanxiao Zhao
Zhifang Wang

Virginia Tech

Aaron Brantly
Alan Michaels
Brian Hay
Cameron Patterson
Charles Clancy
Chen-Ching Liu
Daphne Yao
David Simpson
Ed Colbert
Gretchen Matthews
Haibo Zeng
Ing-Ray Chen
Jeff Reed
Jin-Hee Cho
Jon Black
Jung-Min Park
Kara Nance
Kendall Giles
Kevin Heaslip
Leyla Nazhandali
Matthew Hicks
Michael Fowler
Michael Hsiao
Nathan Lau
Patrick Schaumont
Peter Athanas
Randy Marchany
Ryan Gerdes
Tam Chantem
Walid Saad
Wenjing Lou
William Diehl
Yaling Yang

William and Mary

Adwait Jog
Adwait Nadkarni
Denys Poshyvanyk
Dmitry Evtyushkin
Gang Zhou
Qun Li