Georgia Cyber Innovation and Training Center

Mission:

The Georgia Cyber Innovation and Training Center is a state-owned facility designed to promote modernization in cybersecurity technology for private and public industries through unique education, training, research, and practical applications.

Vision:

The Georgia Cyber Innovation and Training Center will be recognized as a world-class cyber range and training facility focused on developing the next generation cyber workforce through real-world practice, education, public-private collaboration, and interdisciplinary research in the fields of healthcare, computer science, electrical engineering, mathematics, and robotics.

Goals and strategies of the Georgia Cyber Innovation and Training Center:

I. Education and Training
   - Improve Georgia's cybersecurity education, training, and research infrastructure to enhance public and private sectors in cybersecurity preparedness, while building a world-class workforce.
II. Research and Development
   - Enhance research and development opportunities through leading edge technology.
   - Provide small businesses with the tools to grow and compete by allowing access to technology and education resources through the Georgia Cyber Innovation and Training Center.
III. Cybersecurity and Protection
   - Increase protection and security of public resources and provide efficient and effective response to cyber related emergencies.
IV. Economic Development
   - Heighten Georgia globally as the best place for business through innovation and collaboration with private industry in cybersecurity.
V. Government and Public Infrastructure
   - Deliver safe, secure, and efficient government services through inter-agency cybersecurity teamwork.
   - Build a world-class and cyber secure public infrastructure and utility grid to enhance the quality for Georgia's citizens.

Operations business owners:

- Facility owned by the Georgia Technology Authority (GTA)
- Memorandum of understanding with Augusta University for the day-to-day facility operations
- Location of the Georgia Bureau of Investigation (GBI) Cyber Crime Unit

Operations and cost:

The AFY 2017 Governor's recommendation provides a $50 million appropriation in the OneGeorgia Authority budget, which allows for expedited construction of the facility and ensures that funding does not lapse as the program will span fiscal years. Cash funding also allows for more flexibility to meet the specific needs of the facility in which bonds may be more restrictive.

- $41.5M to construct a 150,000 square foot facility
- $2.1M for staffing
- $1.8M for planning and design, utilities, and marketing
- $4.6M to cover staff and operating costs until the building is fully leased
- Groundbreaking in Spring of 2017 and opening within 18 months

What is cyber and why is it important?

Cyberspace is the inter-reliant network of information technology infrastructures that include the internet, telecommunications networks, and computer systems. This increasingly connected infrastructure contains sensitive information from both the public and private sectors related to individuals' social security numbers, credit cards, and bank accounts as well as government intelligence and private companies' proprietary information. The protection of this data is not just valuable to private citizens, governments, and private industries, but its potential vulnerability is also the target of individuals and entities meaning harm through fraud or theft, known as cybercrime. Examples of these cybercrimes are well documented with recent data breaches. In the Unites States since 2005, there have been 5,249 data breaches made public in which 901,013,077 records were breached. In 2016, there were 501 breaches affecting 4,906,563 records.

What is the Georgia Cyber Innovation and Training Center?

In order to meet the challenges of the cybersecurity reality, Georgia will need a state-of-the-art cyber range, where real-life cyber warfare training and cyber technology development occurs. The Georgia Cyber Innovation and Training Center will be a state-owned cyber range and facility bringing academia, private industry, and government together to establish cybersecurity standards across state and local agencies with the capability to develop and practice protocols for responding to cyber threats. The Center will also be a place to advance the field of information security with leading-edge vulnerability research to ensure reliable and effective practices. The Georgia Cyber Innovation and Training Center will house multiple universities and private industries and will provide training and education. The Center will also provide an incubator hub for cybersecurity startup companies. This concept is designed to challenge cyber professionals and systems in a safe and protected setting in preparation for cyber

incidents and provide a multi-architecture environment for related research. This approach will provide access to a range facility dedicated to cyber simulation to closely replicate real world and theoretical scenarios for collaboration across disciplines, agencies, and businesses in the following ways:

- Facilitating collaborative advanced training for the multiple state and federal agencies and professionals charged with protecting the state's information and resources;
- Allowing professionals to practice threat detection, response, and recovery in an environment that mirrors their actual networks, systems, and technologies, and to implement and test new security strategies without jeopardizing the assets or the public they intend to protect;
- Providing security awareness, training and education, professional development, and cyber workforce development;
- Educating and training local human resource professionals to fill increasing workforce deficiencies in cybersecurity jobs in Georgia;
- Aligning the state's resources with a multi-billion dollar federal investment into cybersecurity;
- Providing the ability to rapidly test and evaluate various security architectures and conduct through user self-service mechanisms and application program interfaces (APIs);
- Providing a cost-effective platform to perform exercises to verify government and business readiness while also refining procedures to optimize business-government partnership's response to an inevitable cyber-attack;
- Providing a cost-effective means for the Georgia government to stay abreast of the technology advances and best-practices in cybersecurity that ultimately can be used to benefit its citizens.

How will the Center be unique?

State-owned cyber ranges are extremely rare. Michigan, Virginia, Rhode Island, and Arizona have state-owned cyber ranges. Texas, California, and Minnesota are looking into the potential of having cyber ranges. The Georgia Cyber Innovation and Training Center will be one of a few state-owned cyber ranges and will offer the ability to leverage state resources like research, infrastructure, and training with private industry to advance cybersecurity efforts. The facility will be unique by offering sensitive compartmented information facility (SCIF) space for sensitive information, training and education, and incubator space for Georgia's start-ups.

- A SCIF or SCIF space is a U.S. Government accredited facility where Sensitive Compartmented Information (SCI) can be stored, discussed, or electronically processed. Primarily government and government-related contractors that require high security have the need for SCIFs. The areas of concern and special attention typically include physical security and hardening, acoustics controls, visual controls, access control, and electromagnetic controls. This space has strict guidelines and must be inspected annually by the US Department of Defense (DOD).
- As related to training, the Georgia Cyber Innovation and Training Center will be unlike any other state-owned cyber facility. All services will be available over open, RESTful HTTP/S APIs that all end users can use to dictate how they want to train their teams and on what schedule, rather than relying on large, top-heavy, centralized engineering teams to do all of the design and development work. This will give users the agility and flexibility they need to adequately address cybersecurity

needs as they arise on their terms, rather than at the speed of the governing authority. Beyond traditional x86, the Georgia Cyber Innovation and Training Center will also offer various other central processing unit (CPU) architectures (MIPS, PPC, ARMv7, ARMv8, SPARC, ETRAX CRIS, and MicroBlaze) as well as field-programmable gate arrays (FPGAs). Training that can be offered in this type of facility includes:

- Information Security Officer and Cyber Analysis Training and Certification
- Information Technology and Information Systems (IT/IS) Risk Management and Leadership Workshop Training
- Cyber Incident Workshop Training and Certification
- Continuity of Operations Planning (Disaster Recovery Planning and Business Continuity Planning) Workshops Certification
- Cloud Security and Mobile Device Security Training
- Supervisory Control and Data Acquisition (SCADA)

- Innovation and incubator space will be vital to the Georgia Cyber Innovation and Training Center. The Center will provide a physical space for testing and development that requires physical presence, specifically for robotics and SCADA systems.

Why Georgia and what are the benefits?

According to the Census' Annual Population Estimates, Georgia is the eighth largest state with over 10.3 million individuals and has grown 6 percent from 2010 to 2016, making it one of the fasting growing states as well. Cybersecurity impacts all of these individuals in some fashion through Georgia's economic development, education and training, workforce, government services, and public infrastructure. The Georgia Cyber Innovation and Training Center will not only serve the state of Georgia's interests, but will benefit from the collaboration of new and existing private industries to meet its strategic goals and objectives. The Georgia Cyber Innovation and Training Center will conduct research, training, education, exercises, and testing in protection, detection, and cyber incident response for the state and the nation's critical infrastructures.

- **Georgia's Workforce:** Georgia's labor force is currently over 4.9 million individuals and is growing at a rate of 6 percent since January 2011 (which exceeds the U.S. rate of 4 percent). In addition, current employment in critical cybersecurity sectors make up approximately 35 percent of Georgia's employment. This does not include the signs that show demand for cybersecurity professionals outpacing supply. The 2015 Cybersecurity Jobs Report stated that job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall. It takes companies longer to fill cybersecurity positions than other IT jobs, and Georgia is among the top ten states for cybersecurity job postings. With the Georgia Cyber Innovation and Training Center in collaboration with Georgia's educational system Georgia will produce a cyber-workforce that possess the cyber knowledge, skills, abilities, and tools necessary to protect and defend our information assets, systems, and networks for Georgia and its companies. The Georgia Cyber Innovation and Training Center will produce a cyber-ready workforce through awareness, preparedness, and resilience.
- **Economic Development:** Experts have warned that 90 percent of businesses are victim to at least one security breach, making threats from cyber-attacks near inevitable. According to the Bureau of

Labor Statistics (BLS) and the Georgia Department of Labor (GDOL), Georgia has over 290,000 establishments across 42 major industries and all are vested in cybersecurity or can be considered cyber businesses.

- The Banking and Financial industry is an example of an industry that plays an important role in Georgia and is a target of known and unknown cyber threats. According to the Department of Homeland Security's (DHS) testimony to the House Committee on Financial Services (September 2011), the Banking and Financial industry has become an integral aspect of everyday life providing critical deposit, consumer credit, and payment processing services that face both recognized and unidentified exposures. DHS has indicated that these vulnerabilities are not static, but are expanding due to the malicious adversaries' capabilities in cybersecurity, and the financial industry would be significantly impacted by a lack of communication in cybersecurity. According to Georgia's Department of Banking and Finance, Georgia has over 301 banks and credit unions headquartered in Georgia with another 1,287 banks, mortgage entities, money transmitters and sellers of payment instruments, and financial technology (FinTech) companies doing business in Georgia.

- Additionally, Georgia is quickly becoming a leading center for network and cyber-related industries, which generate more than $4.7 billion in annual revenue; and is one of the largest and most diverse technology industries in the nation with major strengths in health IT, medical devices, software development, and digital entertainment. Georgia is also home to five of the Cybersecurity 500 world's most innovative cybersecurity companies. These companies include: SecureWorks, which uses cyber threat intelligence to provide predictive continuous and responsive protection; Pindrop Security, which provides enterprise solutions that help prevent phone-base fraud; NexDefense, which provides automation and control system operators in critical infrastructure and defense facilities; Ionic Security, which provides data privacy and protection; and Damballa, which is an automated breach defense company that delivers information about known and unknown threats. These companies, combined with the state-owned Georgia Cyber Innovation and Training Center, will place Georgia at the forefront of cyber practices and will vastly enhance the state's ability to attract more information security companies to the state. This focus will help Georgia maintain its ranking as the "#1 state for business."

- **Government Services:**
  - GTA will be owner of the facility and will offer the Georgia Cybersecurity Academy. The academy will initially provide cybersecurity awareness, training, and education to information security officers in state agencies. It is an important new component of the state's strategy for responding to the growing threats from cyber criminals, and its establishment is one of the recommendations from the 2016 Senate Study Committee on Data, Security, and Privacy. Nine courses will be initially offered in 2017 through classroom instructor-led training and online through virtual instructor-led training at the GTA Learning Center.
  - The Georgia Internet Crimes Against Children Task Force, housed within the Georgia Bureau of Investigation's Child Exploitation and Computer Crimes Unit, works to assist state and local law enforcement agencies in developing an effective response to cyber enticement, child pornography and the commercial sexual exploitation of children. The Center will expand on

current initiatives and will provide opportunities for a closer alliance between GBI and, federal, state, and local law enforcement agencies working to identify cybercrimes. The facility will provide GBI the opportunity to train future agents and staff in the newest methods of cybercrimes while in a safe and secure environment. Additionally, the state will develop a GBI Cyber Crime Unit to be located at this facility.

▪ The Governor's Office of Workforce Development (GOWD) in partnership with the Georgia Department of Economic Development offers wonderful opportunities through its Workforce Innovation and Opportunity Act (WIOA) grants to Georgia's citizens looking to obtain education and training in multiple fields. This partnership, along with the Technical College System of Georgia (TCSG), and the approved network of providers allow Georgia to recruit prospective students and retrain the current workforce to pursue multiple diploma, certificate, or degreed programs in order to fill these positions. GOWD has hundreds of approved providers and training programs and the infrastructure to reach any Georgian irrespective of background or financial barriers.

Why Augusta?

Augusta is home to the United States Army's Cyber Command (Fort Gordon), the US Army Cyber Center of Excellence and the National Security Agency (NSA) (representing all branches), making Augusta the destination for cyber professionals in any stage of their career. The US Department of Defense plans to invest $2.1 billion on the construction of the new Cyber Command Headquarters. Centrally located to enhance partnerships across the University System of Georgia (USG) and TCSG, Augusta offers the opportunity to foster collaborative efforts given the scope of professionals required which include computer scientists, computer engineers, electrical engineers, journalists, linguists, business, and health, etc. Augusta University (AU) is a Center of Academic Excellence in Cyber Defense Education as recognized by NSA and the Department of Homeland Security (DHS) and most recently, AU entered into an articulation agreement affording NSA language professionals the opportunity to attain a bachelor's degree while here in Georgia. Additionally, Georgia is already home to one of the ten cyber protection teams with the Army National Guard.

Augusta also provides a unique opportunity to place the Georgia Cyber Innovation and Training Center on state-owned property adjacent to the Augusta University Riverfront campus which provides several benefits to include:
▪ Co-locating the academic institutions responsible for producing DOD Cyber workforce with the operational component actually conducting cyberspace operations;
▪ Creating conditions where academia, industry, and federal agencies can converge to lead in cyberspace security and develop the local workforce to meet exponential demand;
▪ Accessing enormous human capital afforded by the growth from the federal cyber mission and investment coming to Augusta;
▪ Capitalizing on current partnerships to include the National Security Agency who chose Augusta as their home for one of only four nationally focused, mission critical operations centers, known as Cryptologic Centers;

- Creating a training and educational symmetry between federal and state cyberspace professionals in order to strengthen communication, standards, mission support, and enhanced partnerships.

Augusta also offers the Alliance for Cybersecurity Education (ACE) program. The mission of ACE is to utilize the talents, skills, technology, and education and community partners to develop a defined curriculum related to cybersecurity for grades 6-12, which will create a pipeline through post-secondary education and into final employment. Part of this is through teacher/faculty preparedness programs relative to cybersecurity curriculum and identifies appropriate technology resources to support cybersecurity curriculum.

What is the education and training component?
Education and training are essential in cybersecurity, and growing Georgia's workforce related to cybersecurity must be a focus in attracting private industries to the state. According to the 2015 Cybersecurity Jobs Report, over one-third (35 percent) of cybersecurity jobs require an industry certification, and 84 percent of cybersecurity postings specify at least a bachelor's degree, and 83 percent require at least three years of experience. Because of the high education and experience requirements for these roles, skills gaps cannot easily be resolved though short-term solutions. Employers and training providers must work together to cultivate a talent pipeline for these critical roles.

The Center would serve as the pipeline for these critical roles. Modern cybersecurity challenges span disciplines—from computer science to engineering, business and health information, among many other fields. TCSG currently offers diplomas, certificates, and degrees in high demand industry clusters related to Science, Technology, Engineering, and Mathematics (STEM) across its 22 institutions. With recommendations from the 2014 Governor's High Demand Career Initiative (HDCI) report, TCSG offers Strategic Industries Workforce Development Grants (SIWDG) to cover the full cost of tuition for those seeking diplomas and certificates in high demand industry clusters. These industry clusters include 102 programs related to Information Technology and 88 related to Defense. In partnership with the Georgia Cyber Innovation and Training Center and existing offerings, TCSG would be able to expand its current cybersecurity programs located at eight campuses throughout the state.

In addition to TCSG's existing resources, USG has seven institutions that are designated as National Centers of Academic Excellence in Cyber Defense. The NSA and DHS co-sponsor the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program, which is designed to use higher education and research to produce professionals with expertise in the field of cyber defense. These seven institutions include Armstrong State University, Augusta University, Columbus State University, Georgia Institute of Technology, Kennesaw State University, Middle Georgia State University, and the University of North Georgia.

- Armstrong State University and their Center for Applied Cyber Education (CACE) offers numerous cyber degree options ranging from minors to graduate studies.

- Augusta University has a 9,000-square-foot Cyber Institute with Lab to offer cybersecurity courses and degrees that include cybersecurity programs in medical informatics focused on protection of health information and courses on cyberterrorism.
- Columbus State University has the Center for Cyber Defense Education, which was created in cooperation with local industry and offers a Master's of Science in Applied Computer Science with a concentration in Cyber Defense.
- Georgia Institute of Technology provides cybersecurity research and educational outreach through its cybersecurity institutes, labs, and centers and has been awarded a federal $17.3 million cybersecurity research contract to help establish new science centered around the ability to quickly, objectively, and positively identify the virtual actors responsible for cyberattacks, a technique known as "attribution."
- Kennesaw State University, as part of a pilot project to create a certification for Cybersecurity Instructors, will be sponsoring 25 Metro-Atlanta high school teachers with experience in teaching computer-based classes, as part of the Entry Level Certified Cybersecurity Instructors (CCI-E). The program will consist of an online course (Massive Open Online Course – MOOC) on "Cybersecurity and its 10 Domains," and continue with an on-site two day workshop where participants will receive additional cybersecurity and security awareness instruction, including how to create, organize, and conduct cybersecurity curriculum.
- Middle Georgia State University offers a Bachelor of Science in Information Technology with a concentration in Cyber Forensics. The program teaches the digital forensics process of acquisition, analysis, and reporting. The Middle Georgia State University's Center for Cybersecurity Education and Applied Research works to educate the future cybersecurity workforce and provides consultation to local businesses, governmental units, and interested parties.
- The University of North Georgia's Center for Cyber Operations Education prepares students for military and civilian careers in cybersecurity, cyber operations, and cyber defense. UNG offers one degree concentration and two minors in information assurance and security (IAS) and cybersecurity.

In addition to USG's seven institutions that are designated as National Centers of Academic Excellence in Cyber Defense, the University of Georgia (UGA) and University of West Georgia offer cyber related programs and courses. UGA for example offers a graduate certificate in cybersecurity, and will offer a computer science undergraduate certificate in cybersecurity. The University of West Georgia offers a Certificate in Data Analysis and Evaluation Methods.

Quotes on the Georgia Cyber Innovation and Training Center

Georgia General Assembly:

Lt. Governor Casey Cagle
"I support Governor Deal and his commitment to further establish Georgia as a leader in cyber innovation and security. We have a tremendous opportunity as a state to leverage our resources with our research institutions and military bases, and this collaborative initiative will result in a better trained and equipped cyber force."

Speaker David Ralston
"I applaud the Governor for including this initiative in the amended budget for this critical work around cybersecurity. This will distinguish Georgia as the national leader in this arena. We look forward to working with our state leaders in securing the funding for this opportunity."

State Senator Bruce Thompson
"The Georgia Cyber Innovation and Training Center and the work it will do is a bold initiative that will make a tremendous impact for our state. The Governor's vision supports my recommendations as chairman of the senate study committee on data security and privacy to ensure Georgia is on the forefront of cyber security. Georgia continues to enjoy the distinction of being number one in the country to do business, and I'm confident this aggressive investment will create a sector of unmatched economic growth that will keep Georgia number one."

Congressional Delegation:

Senator Johnny Isakson
"Thanks in large part to the efforts of Governor Deal and our entire Congressional delegation, Georgia has emerged as a national leader in cybersecurity," said Isakson, chairman of the Senate Committee on Veterans' Affairs. "Governor Deal's action will cement Georgia's role as a leader on issues of cybersecurity by prioritizing the construction of a new, state-of-the-art facility in conjunction with the defense department and NSA, as well as with private institutions and the state's universities and technical colleges. The Georgia Cyber Innovation and Training Center will be an invaluable resource to our defense community as well as a boon to our economy."

Senator David Perdue
"Georgia is on the front lines of training the next generation of cyber warriors. Building on the innovative efforts we've seen at the United States Army Cyber Command at Fort Gordon, this new specialized training facility in Augusta will help boost our state's cyber workforce. In the face of ever-evolving attacks, our nation must strengthen its defense capabilities to combat the constant asymmetric threats we face on a daily basis. When it comes to cyber security, I'm encouraged to see Georgia leading the way, and I appreciate all the hard work the Governor and legislature are doing to make this happen," said Senator David Perdue, Member of the Senate Armed Services Committee.

Federal Partners:

National Security Agency
"Having a front row seat in our Nation's battle against adversary cyber threats, we at the National Security Agency recognize a strong partnership between government, academia, and the private sector

is a prerequisite to the victory over an entity that wishes to do us harm in or through cyberspace. The Georgia Cyber Innovation and Training Center will allow our best and brightest, from both the public and private sector, to develop critical relationships in an innovative and collaborative training environment. We laud Governor Deal's strategic vision and decision to build the Georgia Cyber Innovation and Training Center in Augusta. This location takes full advantage of NSA's growing relationship with Augusta University, as well as the Army's Cyber Center of Excellence on Fort Gordon, and Army Cyber Command in the near future. NSA Looks forward to this opportunity to partner with academia, the private sector, and other government entities to help recruit, train, and retain the next generation of Cyber Security experts required to protect our Nation against potential devastating cyber-attacks."

<u>Major General John B. Morrison, Jr., Commanding General, U.S. Army Cyber Center of Excellence and Fort Gordon</u>
"Fort Gordon has always enjoyed a tremendous partnership with the State of Georgia and the Greater Augusta community in particular. As one of very few Army installations with continuing growth, that partnership will continue to have strategic importance. With the establishment of Fort Gordon as the Army's Cyber Center of Excellence and soon as the Headquarters for Army Cyber Command, Fort Gordon will quickly become the hub of Cyberspace Operations for the Army. Investments such as the Cyber Range will not only enable our Nation to maintain its advantage in a highly contested cyberspace domain, it will also allow for the type of partnerships between the Department of Defense, Academia, and Industry that is required to attract, produce, and retain the caliber of workforce necessary to be a global leader in cyberspace operations and cyber technologies. We look forward to the opportunities that this Cyber Range will present to the local community, the State, and the Nation."

State Agency Partners:

<u>General Joe Jarrard, Adjutant General, Georgia National Guard</u>
"With our increasing reliance on the cyber domain, the severity of cyber-attacks to cause catastrophic damage to our infrastructure and erode the public's trust also increases exponentially.   The Georgia Department of Defense, with its cyber capabilities and trained network professionals, looks forward to supporting the Governor's Cyber Range initiative. This effort will further his cyber-security strategy and help mitigate these emerging threats and protect the citizens of Georgia. Additionally, it will not only help develop new and improved measures to defend against cyber-threats but it also establishes a means within our State to build strong and enduring relationships among many different partners to enable us all to quickly and cooperatively respond to critical needs in times of crisis."

<u>Vernon Keenan, Director, GBI</u>
"The Georgia Bureau of Investigation looks forward to partnering with the State to address cybercrimes and the technology used to commit them. The investigation of this type of criminal activity requires specialized processes and capabilities which the Center can provide. It will greatly enhance Georgia's ability to protect its citizens."

<u>Calvin Rhodes, Executive Director, GTA</u>
"Georgia's Cyber Innovation and Training Center will bring together partners from education, government, and industry in a state-of-the-art environment. Collectively, this partnership will make a real difference in cybersecurity for Georgia and for our nation," says Calvin Rhodes, State of Georgia Chief Information Officer and Executive Director of the Georgia Technology Authority. "The Governor's vision for cybersecurity is expansive, with an emphasis on workforce development, a safe environment to train and exercise skills, and a setting that spurs innovation. The center will foster the alignment in

training and technology that we need for the future. It represents a tremendous investment in this state as we all work to strengthen cybersecurity preparedness."

Stanton S. Gatewood, State Chief Information Security Officer, GTA
"Our ability to face emerging cyber threats depends on the right training and the right tools," says Stanton S. Gatewood, State Chief Information Security Officer. "Georgia's Cyber Innovation and Training Center will provide both in a groundbreaking approach. Together, we will develop a cyber-workforce equipped with the education and real-world practice required in a rapidly changing world."

Steve Wrigley, PhD, Chancellor, University System of Georgia
"Governor Deal's cybersecurity initiative represents a strategic investment for the long-term benefit of our state. Cybersecurity is a critical workforce need and several of our institutions have received national recognition for their teaching and research in this important field. We are eager to fully deploy the resources of the University System to help bring the Governor's initiative to life."

Brooks Keel, PhD, President, Augusta University
"The Governor's vision for a facility which will allow the best and the brightest in academia, industry, and government to work together to address global cybersecurity challenges is truly transformational. Augusta is already home to an array of intellectual capital with the establishment of the Army's Cyber Command headquarters in Augusta, and Augusta University's growing partnerships with the Army Center of Excellence and NSAG. Construction of a cyber-range will allow us to provide state of the art training for the cyber workforce that is so desperately needed by industry and our military. I look forward to working closely with all of our partners as we do even more to turn this vision into a vibrant reality."

Jere W. Morehead, JD, President, University of Georgia
"The depth and breadth of the University of Georgia's expertise in cybersecurity and related fields—which ranges from training tomorrow's workforce to conducting groundbreaking research and leveraging the University's statewide infrastructure and networks—will enable this institution to play a key role in this critical initiative," said UGA President Jere W. Morehead. "We are committed to working with partners in government, industry and academia to enhance national security and economic vitality. Working together, we can stay one step ahead of emerging threats and create a more secure future."

G. P. "Bud" Peterson, PhD, President, Georgia Institute of Technology
"I applaud Governor Nathan Deal and his strategic approach to further solidify Georgia as a leader in addressing critically important cybersecurity challenges," said Georgia Tech President G. P. "Bud" Peterson. "This is an excellent opportunity for public research universities such as Georgia Tech to partner in developing solutions for some of society's toughest and most important problems. Georgia Tech stands ready to lend our expertise and support for this statewide initiative."

Gretchen Corbin, Commissioner, TCSG
Commissioner Gretchen Corbin of the Technical College System of Georgia says she applauds Governor Deal's leadership in creating a Georgia Cyber Range and looks forward to TCSG being a partner in its growth. She went on to say, "TCSG will quickly and efficiently provide to this critical program our strongest assets: training programs customized to meet the specific needs of industry, as well as the skilled talent to ensure company growth for years to come. We will partner by offering technical certificates, diplomas and degrees through Augusta Technical College, while bringing the nation's top

economic development workforce development program, Georgia Quick Start, to the table to work with employers as they grow cyber-related jobs in Georgia."

Herbert J. Mattord, Associate Professor, Kennesaw State University
"If you look at the U.S. Bureau of Labor Statistics, they're predicting a 32-percent year-over-year increase in cybersecurity analyst positions. Staffing for cybersecurity jobs already is nearly impossible, given the current circumstances. There simply aren't enough young people willing to learn the skills, and the people who are in the workplace now are commanding great salaries. It becomes increasingly difficult and more expensive to recruit the most experienced candidates. We need to expand the pool of prepared workers. We're starting to see the larger companies becoming more aggressive when it comes to recruiting at the entry level; people are hiring someone with a four-year degree in security and then grooming them for their organization."

Private Sector Partners:

Walter C. Sprouse, CEcD, HLM, Executive Director, Augusta Economic Development Authority
"The Georgia Cyber Innovation and Training Center will be a place for the military, private sector, and academia to collaborate and create solutions to current and future cyber issues. Fort Gordon is the new Power Projection Platform in information dominance for the United States. This facility will be a key part in supporting that mission through research and training the workforce of tomorrow. The Augusta Economic Development Authority is proud to play a key role with the State of Georgia, Augusta University, Fort Gordon, and all who keep our Nation and networks safe."

Renee Lopez-Pineda, Director, Cyber Security, Delta Air Lines
"The state's dedication to collaborating with industry on cybersecurity training, research and innovation will give Georgia companies another avenue to expand cyber training efforts. That's good for business and customers in Georgia, and beyond."

Bill Leahy, President, AT&T Georgia
"Within the past year alone, 689 million people in 21 countries experienced cybercrime. In fact, AT&T has intercepted more than 2.5 million malicious messages and cyber threats in a single day, and the Georgia Cyber Innovation and Training Center will provide an unparalleled opportunity for cyber professionals to test their skills and systems in a safe and protected setting. This kind of real-world practice will be invaluable in training a new generation workforce as well as providing educational opportunities for our current workforce. Georgia's strong and diverse economy is attractive to cyber-criminals, and the Governor's commitment to advancing cyber-crime fighting capabilities is something all of us can support."

Randal Robison, Chief Information Officer, Georgia Pacific
"Cybersecurity is a growing concern for industry, government and every individual. Preparedness for future challenges will require just the sort of collaboration, multi-disciplinary research and education that Georgia's Cyber Innovation and Training Center can provide."

Avi Rembaum, Vice President, Security Solutions, Check Point Software
"Ultimately, a center of innovation needs to reach a point of critical mass – where companies, organizations and government work together as an ecosystem to drive new growth….It's around that continued momentum; much of that needs to be built on a culture of innovation and creativity, and

making sure that business, education and government work together in fostering that continued growth."

Robert Skiba, Executive Vice President, InComm
"As the world finds itself having to deal with the realities of a 'Cyber Planet', Georgia finds itself at the Center of America's FinTech & Mobility Sectors and it is uniquely positioned to form a coalition of academia, private industry and government resources to become the global locus for 'All Things Cyber'! With a longstanding Global Mobility Center and approximately 100 Georgia based FinTech Firms located in Georgia, with about 90 Firms located in Metro Atlanta – alone, Georgia will process in 2016, more than 70 percent of the $5.3 trillion in U.S. FinTech payments, in what has been called 'Transaction Alley'. In addition, Georgia has huge existing Cyber Security presence. The state of Georgia leads the nation in the Information Security industry, with research, academic resources, talent and a number of data centers. Georgia is now home to more than 115 information security companies, which generate more than 25 percent of the worldwide security revenue market. Given the major existing Georgia based Cyber & FinTech firms, academic resources – research, U.S. Cyber Military Operations (Fort Gordon) and supportive Georgia State & Federal Government Leadership, it is critical to develop a Georgia Cyber Range – to coordinate these valuable assets, talent, resources and make Georgia the Cyber Center of the World!"

Tee Green, Executive Chairman, Greenway Health
"I applaud the Governor for taking such bold action in launching the Georgia Cyber Range. Our ability in GA to train cyber professionals in such a coordinated manner will put GA at the forefront of cyber initiatives. This will enable our companies to partner with the best and brightest right here at home which will give GA companies a great competitive advantage on the global stage."

Tom Miller, Chief Information Officer, Anthem
"Anthem certainly supports this progressive initiative by Governor Deal and the State of Georgia, and would be honored to participate in the discussions and strategic planning. We recognize Georgia's exceptional position in terms of technology resources, which is exactly why we decided to locate Anthem's major technology hub in Atlanta. Collaborating on cybersecurity is a natural extension of that base of expertise."

Robert Varnadoe, Chief Information Security Officer, NCR
"As NCR continues to grow and expand our global software, SaaS, and services business, expanding the pool of trained talent with cyber security proficiency is critical. Georgia's announcement to invest in the Georgia Cyber Innovation and Training Center will help businesses like ours meet our future needs to train and educate a cybersecurity workforce right here in Georgia."

Anil T. Cheriyan, Corporate Executive Vice President, Chief Information Officer, SunTrust Bank
"We recognize that cybersecurity is a concern and we have invested significant resources to help protect our organization against these types of threats. We also work with industry and government entities to stay well informed and help reinforce those efforts. Protecting the safety and security of our systems, and the client information entrusted to us is paramount. We have extensive multilayered security protocols and processes in place to help ensure we protect our clients and SunTrust."

Paul Bowers, President and Chief Executive Officer, Georgia Power
"In order to protect those they serve, businesses, government agencies and the military have increased their focus on effective cybersecurity," said Paul Bowers, Georgia Power chairman, president and CEO.

"Fort Gordon is already home to the Cyber Center for Excellence and this new cyber command headquarters will build on the existing network in Augusta to significantly improve defensive measures that protect important digital resources. When completed and operational, these facilities will put Georgia at the forefront of cybersecurity, while expanding protection offerings for the public and private sectors."

Dent Thompson, Vice President and Chief Operations Officer, Phoenix Air Group, Inc.
"Phoenix Air Group, Inc. is headquartered in Cartersville, GA and is a worldwide operator of aircraft supporting various special missions around the world for the U.S. Department of Defense, U.S. Department of State, and other government and private sector organizations. Cyber security is a major concern to us and we constantly work with our federal partners to develop and implement the latest and very best cyber security practices, but this is a moving target since those who would seek to gain entry or harm companies and organizations through cyber hacking are constantly evolving and changing their tactics. As a Georgia-based company, we support and salute the Governor and State Legislature for local efforts to develop and bring to Georgia industries best practices and training in the field of cyber security."