NWX-DOC-NTIA-OTIA

Moderator: Francine Alkisswani
April 17, 2019
1:00 pm CT

Coordinator: Welcome and thank you for standing by. All parties are in listen-only mode for today's conference. At this time I'd like to inform all parties that today's call is being recorded. If you disagree you may disconnect at this time. Thank you and you may begin.

Francine Alkisswani: Good afternoon everyone and thank you for joining us today for Broadband USA's monthly webinar. My name is Francine Alkisswani and I am a telecommunications policy analyst with NTIA's Broadband USA. Today's webinar HBCU Model Programs and Practices for Building a Competitive Cybersecurity Workforce will highlight educational programs that address training for cybersecurity professionals focusing on contributions made by historically black colleges and universities, HBCUs.

You will also learn how the Minority Cybersecurity Council is working to bridge the gap between industry, government and education in order to inform the minority community about the growing employment and training opportunities in cybersecurity. Our presenters today are Karl Cureton, Executive Chairman, National Minority Technology Council and Executive Director Minority Cyber Inclusion Council, Dr. Kevin Kornegay, Professor

and IOT security endowed Chair, Director of Cybersecurity Insurance and Policy Center and Director, Center for Reverse Engineering and Assured Microelectronics, Morgan State University. And Dr. Aurelia Williams was the Executive Director of the Cybersecurity Complex and Lead PI for the Consortium Enabling Cybersecurity Opportunities and Research, Norfolk State University.

Our moderator today is Dr. Bruce Berger who is the Lead for the HBCU Cybersecurity Cluster and Director, Center for Innovation and Entrepreneurial Development at Clark Atlanta University. Now I would like to give the logistics for today's webinar.

First we will open up the webinar for questions after the completion of the presentation. So as you hear from each presenter please use the question box on the right hand side of the screen to submit your questions or comments. Second, these slides along with the transcript and audio recording of today's session will be available on the BroadbandUSA website within seven days of this webinar.

You'll find it under the Events/Past Events tab. And finally we'd like for you to please visit our BroadbandUSA website for information about our technical assistance programs including useful guides, products, publications and other tools that can assist you with planning, funding and implementing your broadband project.

So as we begin I would like to introduce our moderator, Dr. Bruce Berger. Dr. Berger presently serves as the Director of the Center for Innovation and Entrepreneurial Development and media lab at Clark Atlanta University. He graduated from the Wharton School of Finance and Commerce Tech University of Pennsylvania with a BS in Economics and later entered -I'm

sorry, later earned an MBA and JD degree at the University of Miami and the University of New Hampshire, Franklin Pierce Law Center respectively. So he brings a complex of skills and perspectives to this moderation task so I will now hand it over to Dr. Berger.

Bruce Berger: Thank you Francine and good afternoon to our audience. And I'm told we have about 300 registrants today so congratulations to you folks brave enough after lunch to go through this wonderful exercise today.

Although Voltaire once stated I was never ruined but twice, once when I lost a lawsuit and once when I won one. I will not let the fact that I am a lawyer obstruct, obfuscate, or otherwise ruin our having an enjoyable time today. And thank you on behalf of our distinguished panel to BroadbandUSA and the NTIA for inviting us to be here with you today.

Please allow me to level set today's discussion on HBCUs and building a competitive cybersecurity workforce. Today's webinar is simply about opportunity and the value propositions that HBCUs bring to this space. Many of you know about some of our leading universities with R&D capabilities for developing cutting edge broadband and cybersecurity technology and for graduating top talent who will become leaders in these fields.

But how many of you are familiar with some of our great historically black universities and colleges, HBCUs, especially those who have some of the same capabilities as MIT, Stanford, Carnegie Mellon, Georgia Tech and other notable higher Ed institutions. Our HBCUs have a rich history of developing innovative technologies and producing the most black educators, doctors, lawyers, pharmacists, physicists, dentists, judges and university presidents.

And in a few moments you will hear about two HBCUs that are at the forefront of a national imperative, cybersecurity, which will bring you to the inescapable conclusion that the HBCU value proposition is on par with those great institutions I just mentioned. But first please indulge me in a brief HBCU history lesson.

Historically black colleges and universities are institutions of higher learning that were established prior to 1964 with the principle mission of educating black Americans. These institutions began in the 1800s and were founded and developed in the environment of legal segregation. The first one in fact was founded in 1837, now Cheyney University of Pennsylvania by a Quaker and a Philadelphia philanthropist as a trade school for African Americans. It was called the Institute for Colored Youth.

HBCUs have made an indelible global imprint on virtually every facet of culture and society. HBCU alumni have ascended to leadership positions in government, education, business, industry science, technology, medicine, literature, entertainment and every other imaginable profession and vocation. The rich and lasting heritage of these institutions is the testimony to their resilience and unremitting commitment to providing access to higher education for African-Americans and others seeking empowerment and expanding their opportunities with a college degree.

There are 101 HBCUs located in 19 states, the District of Columbia, and the U.S. Virgin Islands and the contiguous U.S. states as far west as San Antonio and as far north as Pennsylvania and as far south as Miami. These 101 offer, 27 of them offer doctoral programs, 52 schools offer master's program and 83 colleges offer bachelor's degrees and 38 schools offer associate degrees. Although HBCUs were originally founded to educate black students they

enrolled students of other races as well especially those unable to afford state tuition.

This diversity has increased over time and in 2017 non-black students made up 24% of enrollment at HBCUs compared with 15% in 1976. In fact, one HBCU in West Virginia is predominantly white and has been for decades as many blacks have abandoned Appalachia. Female enrollment at HBCUs has been higher than male enrollment in every year since 1976. The percentage of female enrollment at HBCUs increased from 53% in 1976 to 61% in the fall of 2017.

In the academic year 2016/17 some 49,500 degrees were conferred by HBCUs. Of the degrees awarded at HBCUs the majority or 74% were conferred to black students. HBCUs responsible for 22% of current bachelor degrees granted to African Americans. That's 1 out of 5. If we consider the impact of HBCUs by occupation according to the *Network Journal* of the African American represented in the workplace 40% of our members of Congress, 40% of engineers, 50% of lawyers, 80% of judges graduated from HBCUs.

So now let me turn to the slide that's on the screen that HBCUs, first of all, are national strategic assets you can see at the top box about 12:00 high, not solely because they serve a minority population but because they are dedicated to serving the -the underserved communities -- which is on the left side at about the 9:00 position. You know as well as I that we have underserved and disconnected communities, disconnected from the 21st century innovation economy, both the urban and to be fair rural but who is better positioned to facilitate the capacity building and the infrastructure building in these communities, many of whom like my institution Clark Atlanta University and southwest Atlanta are in opportunity zones. Therefore,

we become the anchor institutions to develop research and innovation, spur entrepreneurship, see the bottom box right there at 6:00, and curate a qualified inclusive and competitive workforce in broadband 5G spectrum cyber physical systems.

And so at the 3:00 position, you know, we have also this discussion about excellence in cybersecurity and getting the workforce ready. HBCUs as mentioned have a history of research and innovation. They are a proven economic engine in the communities they serve. In fact, the United Negro College Fund, the UNCF, released a study calculating to total economic impact of 100 historically black colleges and universities at $14.8 billion.

You will hear today in a few moments that HBCUs are on the cutting edge of research and have the capacity to enhance their local economy and are one of our nation's key resources for diversity and inclusion in our workforce pipeline. With a level playing field for HBCUs to receive grants and more importantly contracts to attract public/private partnerships, to create opportunities on businesses and to build community economic development, these capable and highly competitive anchor institutions strategically located and poised to innovate are really opportunity hubs for diverse and inclusive cyber workforce and building HBCUs cyber consortia, as stated in the bull's eye of the slide, is really the sweet spot for robust opportunity to prevail. So in my conclusion here, HBCUs are a vital source of change and growth for our economy. It is my true hope that this webinar will inspire university faculty and administrators to seek new partnerships and research opportunities to encourage industry and business leaders to reach out to their local HBCU counterparts to partner and to innovate together to encourage HBCUs to develop these consortia level partnerships with each other and with other qualified universities, with industry, with government and with non-profit

constituents and to encourage parents and students to look at HBCUs as an answer to help prepare them for a meaningful career.

Our first speaker is Karl Cureton. Karl is the Founder and Chairman Emeritus of the National Minority Technology Council. Karl is the Founder and Chairman Emeritus of the National Minority Technology Council and the Managing Director for the Minority Cyber Inclusion Council. NMTC recently merged with the Council Exchange Board of Trade, a Virginia non-stock corporation registered with the IRS as a 501c6 business league, representing the now over 65,000 U.S. based minority technology employers. Let me repeat that, 65,000 U.S. based minority technology employers.

Karl also serves at the Chair of the Board of Directors for the Virginia Career Education Foundation. This man is a wealth of knowledge in this particular field. I hope you enjoy. Please welcome Karl Cureton.

Karl Cureton: Thank you and it's an honor on this BroadbandUSA April webinar representing the National Minority Technology Council and the Cyber Workforce Program we're calling the Minority Cyber Inclusion Council. I wanted to acknowledge the National Telecommunication Information Administration for its leadership in governing spectrum and the future of 5G and for allowing Dr. Francine Alkisswani to detail last year with the White House initiative for HBCUs.

Her commitment to collaboration and excellence is noteworthy and our industry -and at our industry association we're always ready to celebrate excellence in government. Also Bruce that was a great recap of the HBCU story. Thank you. Indeed historically black colleges and universities are from our longitudinal research, the nexus point for intervention -for intervention

research and discovering with regards to solving the workforce shortage crisis in cybersecurity.

It's critical we intentionally build and model programs and practices that enable a more competitive and inclusive cybersecurity workforce. Doing that not only works to ensure opportunities for all but it provides our nation with a strong defense against threats and begin to build a more resilient nation. Next slide.

I am tasked today to discuss our Minority Cyber Inclusion Council. For those like me who always have more than one screen going at the same time you can look ahead at the program website, www.mcicouncil.org, while I'm talking. Our vision is that to build an inclusive cybersecurity workforce or perhaps make this unique if the employer input and focus we bring to our program design.

I'll go in more detail about our research methodology and program design but first let me give you some context for our industry research, the next slide. As a point of reference the National Minority Technology Council started 20 years ago and now stands aligned with the Council Exchange Board of Trade, as Bruce said a Virginia non-stock corporation registered with the IRS with the 501 business league, and again we represent these 65,000 minority technology companies; but minority technology company employers provide solutions every day.

In fact, if you add up the sales of the 65,000 minority tech companies you'll be looking at 100 billion in gross receipts per year. So that's 100 billion in sales per year and they employ over 500,000 people, many in the cybersecurity sector. What are more exciting area of development is the creation of an opportunity fund to invest in the new opportunity zones. From

our perspective it's critical that industry takes the reins in developing disenfranchised communities for both workforce readiness and for public private investments in new infrastructure. We believe in a nation that we're strong together and as technologists we bring critical thinking and jobs to the ecosystems we serve. Next slide.

The Minority Cyber Inclusion Council is part of our looking forward research and development directly. Our theory of change is together we make the change. From our research what is in the way of growth is more hazard and information of symmetry. To that end our mission aligned is on the following outcomes.

We want to increase the public/private research and technology transfer particularly in partnerships with HBCU and MSI anchor institutions. Just for a reference point federal research is $150 billion a year and minority tech companies are doing about 5%, huge growth opportunity. Increase in both grant and contract funding for our stakeholder partners, again a reference point between public and private universities.

Over the last ten years there's been $124 billion of federal contracting. HBCUs have received a billion, huge upside potential for HBCUs, increase in connectivity to bridge building that includes old fashioned one-on-one discovery requirements discussion. We believe that talking to each other is the best point of reference, the result is increasing wage and increasing individual wealth which is so vital in our minority communities and leads us to better outcomes to wellbeing. Next slide.

This next slide is our stem cortex framework that outlines our research program component. As we develop initiatives like the Minority Cyber Inclusion Council we utilize this framework. As you can see we embrace

complexity as a corporate culture. The iterative nature of innovation creates ideas, experimenting, testing and learning. It's so important that we understand that complexity is cool. Next slide.

The Minority Cyber Inclusion Council was developed in part to build an alliance between minority technology industry Title I schools particularly in middle school and higher education. As a trade association we see universities in particular HBCUs as a strategic world resource for community growth. Our general proposal is for HBCUs to consider the value of applied research.

This research methodology used to solve specific practical problems. In fact, two distinguished HBCUs presenting today have, and you'll see, a function utilizing this methodology. This type of research is exciting, engaging particularly with cybersecurity. It attracts business owners and corporations to your campuses, assists faculty and student retention and allows relevant industry discussions that may lead to industry investments both time and money. So consider applied research. Next slide.

From our research great many HBCUs are already ready for change. Both large and small universities are engaged in developing projects that will build future revenue and increase student achievement and allow for better learning environment. The future is bright. In fact, we see an increase in private investment partnerships with HBCUs over the next decade. Particularly consider the impact of this new path law and creating opportunity zones and opportunity funds. Next slide.

Partnership matters, relevant partnerships last so partnerships matter but relevant partnerships last. I hope it's not lost in the listeners today that part of the theme is the expansion of 5G and the growth of the Internet of Things.

The 5th generation of wireless technology promises lightning fast speed, low latency and the capacity to carry massive numbers of connections simultaneously. 5G will offer a multitude of benefits but will also come with risk.

That's the increased number of devices, elevated use of virtualization, software design network, the Cloud. It's just, you know, there's a lot of things happening in a broader met multi-faceted attack surface. You're going to hear more about that today. Industry recommends HBCUs take a leadership role in developing research partnerships to explore new strategies to enhance our nation security positions. Next slide, next slide, thank you.

Federal government is onboard and full force. The Federal government recognizes and is putting resources to bear to encourage innovation at the HBCU level. This is occurring in multiple agencies and this Trump Administration is focused on cross agency collaboration. For those in academia listening I encourage you to consider establishing partnerships and consortia as Bruce said that middle target slide, to better attract and win both grants and contracts. This discussion today is a national imperative. Next slide.

We are finding out more and more how AI is going to eliminate the need for a host of jobs in the future. Cybersecurity has the opposite effect. There's an estimated 1.5 million net new jobs in cybersecurity within the next five years. This is a windfall for minority community. Simply put, cyber pays. Next slide.

Over the past six years the National Minority Technology Council has conducted independent research to develop methodologies to best enroll and adopt students in the business focused ecosystem that allows for subject

matter experts in university, government, large commercial act organizations access to new recruits who are aware of the work role required to enter and stay in the workplace. At the core is the rationale that private and public sector partnerships need to align education and training with employees, for the employer cybersecurity and workforce needs.

The slide here is talking about last year the Minority Cyber Inclusion Council was listed in the U.S. Department of Commerce National Institute of Standard Technology, NIST, National Initiative for Cybersecurity Education, NICE, workforce management sub-working Group Paper called Cybersecurity is Everyone's Job and the organization illuminated as a cyber organization representing minority population. Next slide.

Our initial focus is on - the analyze and oversee - cyber framework specialty area; and we got this information from cyber seek, a great resource you can find at www.cyberseek.org. This website shows these two specialty areas have a current demand of over 212 jobs, 212,000 jobs - current demand.

The core design framework for cyber of our curriculum development and badge level certification is the NIST NICE cybersecurity workforce framework. Next slide.

Okay so the academic listeners today or academia listeners today, our approach to learning and workforce readiness is more trans-disciplinary. That's to say our methodology for academic engagement transcends disciplinary. This approach brings a more comprehensive framework that crosses boundaries of both academic and public and private spheres.

It's our view that mutual learning, joint work and knowledge integration are key to solving real world problems back to the applied research. Building

virtual construct where students and faculty bring experimental applied research, combining multiple campuses, disciplines and public private sector. Next slide.

Thank you for listening. For those who heard something important and want to follow up, feel free to go to our website www.mcicouncil.org. If you'd like to know more about just the council, www.mtcimpact.org. Thank you again NTIA and U.S. Department of Commerce for this opportunity to share our progress and Bruce. That's all I have for today. Next slide and you can take it from here.

Bruce Berger: Thank you very much Karl. You have certainly stated the case for diversity and inclusion and building a competitive cybersecurity workforce in the broadband and cybersecurity economic ecosystems which leads us to our next two speakers, both of whom are subject matter experts in cybersecurity, cyber physical systems and broadband IOT networks and who just so happened to be esteemed professors and colleagues at HBCUs.

So first up is Dr. Kevin Kornegay who received his BS degree in Electrical Engineering from Pratt Institute in Brooklyn, New York and his Master Degree and PhD degrees in Electrical Engineering from the University of California at Berkeley.

He is the IOT security professor in the Department of Electrical and Computer Engineering, Director of Security Assurance and Policy Center and the Director of I love this name, CREAM, the Center for Reverse Engineering and Assured Microelectronics Laboratory at Morgan State University in Baltimore, Maryland. Please welcome Dr. Kevin Kornegay.

Kevin Kornegay: Thank you for that wonderful introduction and good afternoon folks out in the audience. It is indeed a pleasure for me to present to you some of the work that we're doing, the exciting things we're doing at Morgan State University. First slide please.

Okay. So 5G has a lot of advantages that will assist us and prove a quality of life across many levels. In particular it is intention -intended to provide ubiquitous connectivity of every device. So everything's going to be connected to everything and it will impact our daily lives in a profound way and so -but it would also create tremendous opportunities, new opportunities for adversaries. Next slide.

So with the how's it going to impact our lives in a variety of ways, this chart is a very good depiction of you know, the technologies that are all interconnected. You have a wide variety of different wireless standards. So everything's going to plug into 5G which will be the backbone for distribution. So there will be tons of data but the point here is that all of these devices and I can say which was considered IOT devices, they will be connected and an adversary will have a field day with this type of broad expansive network. Next slide please.

So to address some of the cyber issues one of the jobs that we one of our primary functions is the subject to the assurance of policy center on the research side is to protect our critical infrastructure from exploitation by bad actors, and so we formed this center that has two roles. It serves as an education center so where cybersecurity, a center for academic excellence is the cybersecurity defense as designated by the NSA and the Department of Homeland Security.

And then there's a research focus and the cap is sort of the overlap of education and research. So our goal is to eventually to be subject matter experts who have a tremendous impact on educating the community about you know, best practices for example, how do you configure your IOT devices to be as secure as possible. Impact on our economy in terms of the product development, training, production of PhDs and the actual level cybersecurity highly trained and skilled cyber engineers.

So ultimately it becomes sustainable over time so that the funding that we see from the state, we don't become totally reliant on soft money. Next slide please.

So the vision of the center in the state of Maryland the cybersecurity ecosystem, per se, there are only three universities that have the highest designation bestowed upon them for an academic institution and that's the Center for Academic Excellence and Research where they focus in some sort of thrust in cyber research -cyber security research and those three universities are University College Park, Johns Hopkins, and University of Maryland Baltimore County.

However of the 14 -there are 14 CAEs and CD centers in the state of Maryland, only -as a matter of fact none, there are well over 100 plus of these standards of course in the country in various regions. None of the -there isn't a single HBCU that has the CAE, the research designation. So we want to become the first and we're well on our way to accomplish that but our goal, but our mission is to essentially produce highly skilled cyber security professionals to prevent the penetration and manipulation of our nation's critical cyber infrastructures.

And how we accomplish that is through using a wide variety of reverse engineering techniques, we as reverse engineers work –it is essentially working backwards but we use these techniques to expose vulnerabilities in IOT devices and then we propose that which are points of exploitation; and then we propose mitigation to both measures to mitigate these exploitations. Next slide, please.

So we define an IOT device as a device that performs three primary function. It senses where it interacts with this environment and then it performs some sort of decision or some primary decision on whatever physical quantity or whatever encounter it interprets from its environment; and then it pushes it out to Cloud. So it senses, it processes and it communicates; and an adversary who wants to or bad actor, they will attack the device on one of these three different sectors.

And so to do so you have -students have to have knowledge and expertise and physics and electronics and programming language and communication standards and protocols, etc. So, they have to have this potpourri of skill sets in order to address this. And we do -we've created this very comprehensive unique program at Morgan to impart a lot of those skills to the students. Next slide, please.

So IOT devices and every electronic device for that manner, they leak information particularly during an authentication operation so when you're doing banking on your cell phone. You enter your PIN. There's some form of encryption that goes on between your mobile device and the Cloud and the -it is during that point when it -if you can listen in during that operation. You can have the right equipment. You can kind of -group force at using statistical means to reproduce the encryption key or PIN or password. Next slide, next slide.

So in our -in the laboratory, in the CREAM lab, located in the Schaefer Engineering and Building at Morgan State we have -we create these test beds that represent a wide variety of the typical infrastructure so there's a home/office automation test bed and the smart grid test bed for example; and here is a perfect example where a bad actor can configure a drone.

They can fly it on off to your rooftop. They can hack into your home Wi-Fi system, ease control of your home automation devices, disable your security. They can unlock your doors, et cetera. So they can wreak havoc on your life. Next slide, please.

Our faculty in the center, these are just representatives of the faculty but we have -they have a wide range of skills and expertise ranging from wireless authentication to data analytics and machine learning to software defined radio and hardware assurance and education and outreach. Next slide please.

We have a broad range of sponsors and partners, sponsors who fund an amount of our research that includes National Security Agency, National Science Foundation, IOPA, there's DoD labs, the only research lab, MIT, Lincoln laboratories and so on and Lockheed Martin who is one of our industrial partners.

We also have university partners who we collaborate with on and go after large block funding and they include Dartmouth, Johns Hopkins, the University of Maryland, Capital Technology and Virginia Tech. So these are -we've been able to leverage resources from other universities that complement, provide a comprehensive research platform of -to go after to secure a large block funding. Next slide, please.

With regards to our education, we've also crafted a unique secure admitted systems doctorate program where that imparts a lot of the knowledge that students need that enforces ranging from digital forensics, machine learning, AI, cryptography, hardware reverse engineering and so forth. Next slide.

And here is a list of the types of skills, kind of arranged in four different categories, cryptography, hardware assurance, software. So this is just a list of some of the skills that the students acquire over time. Next slide.

Presently we have -of the Cap scholars we currently have 13 doctor engineering students. We just graduated first doctor of engineering student who went through the program this past December. One thing that's unique and this is in -this is a unique characteristic that every HBCU brings, is that the percentage of -of the 80/20 rule was 70/30 rule but at least 70% of our -these doctoral students are U.S. citizens.

And we also have a large percentage of those are women, 5 women. And that's unique in that regard in these times where women are underrepresented in the computer science and the STEM field and (unintelligible). So we offer that, this unique population that's potentially clearable of workforce, this workforce that Johns Hopkins and UMC, University of Maryland College Park, which where they have an 80% international, this is at the graduate level, international group population.

So NSA and folks in DoD cannot -they can't hire those students. The other thing too is that our students are exceptional. They hold a wide range of prestigious graduate fellowships and scholarships including the DoD Cyber Security Scholarship. Next slide.

Lastly, we have a wide range of other degree programs in the cyber area ranging from masters -professor master's degree in cyber engineering. That's a maybe program and these -I have a list of other university wide cyber programs. Next slide. So I'd like to thank everyone for your time and listening to me just talk about some of the exciting things we're doing at Morgan State University, thank you.

Bruce Berger: Thank you Dr. Kornegay, again a great exemplar of the value proposition that HBCUs bring to the table in this cyberspace area. Your presentation was highly informative and illustrates Morgan State University's critical role in the state of Maryland cybersecurity ecosystem. And it also demonstrates how an HBCU is innovating while looking toward the future of IOT device vulnerabilities which is a tremendous national security issue and a frightening one indeed, especially those drones flying over our personal rooftops and stealing all of our information and knowledge. Yikes is all I can say about that one.

So next up our last speaker Dr. Aurelia T. Williams is the Founding Executive Director of the Cybersecurity Complex and Professor of Computer Science. During our tenure as Chairman of the Computer Science Department she led a team of highly engaged faculty to secure $33 million in external funding for cybersecurity activities.

She currently serves as the principal investigator of the consortium enabling cybersecurity opportunities and research, a collaborative project that combines the strength of HBCUs and energy laboratories to positively influence the cybersecurity workforce, again a great example of these cyber consortia that we need to be involved in. But Dr. Williams earned her undergraduate degree in Computer Science from Norfolk State University. Her Master's degree was earned in Computer Science from the Whiting School of Engineering at John

Hopkins University and her doctoral degree was conferred from Pace University in New York. So now I present to you Dr. Williams from Norfolk State University, thank you.

Aurelia Williams: Good afternoon. Norfolk State University located in Norfolk, Virginia is a comprehensive urban public institution committed to transforming student lives through exemplary teaching, research and service. NSU is a university recognized nationally as a coming and public institution with outstanding signature academic programs, innovative research and community engagement opportunity. Next slide, please.

Our cybersecurity initiative began in 2003 with the establishment of our Masters and Computer Science. That included emphasis in information assurance. Our first external award was received by our visionary Dr. Sandra DeLoatch who was designated as the Massie Chair of Excellence for Information Assurance. That program was designed to create a team of world class filers, researchers and educators who advanced research and enhanced academics promote partnership, affect outreach and produce top level graduates in groundbreaking research.

Today we offer a BS and MS computer science programs with emphasis in information assurance on cybersecurity. We also offer an MS in cybersecurity. We developed a proposal for a PhD in cybersecurity and data science and we are also pioneering cyber psychology with the new globally linked graduate degree program that will be effective this fall.

We are also the home of the NSF funded project to infuse cyber modules into new sociology curriculum. NSU has been a leader in K-12 outreach through cybersecurity summer camp. We have been selected as a model designated cyber camp by the Department of Homeland Security. We have also talked

and established the cybersecurity club at IC Norcom High School in Portsmouth, a neighboring city, and our mentorship successfully helped them to write and receive their own grant to hold their own Virginia cyber camp. Next slide please.

NSU has a history of partnering with federal agencies and laboratories, industry and other universities. We currently manage large consortia. We are a national science security agency, Department of Homeland Security Center of Academic Excellence and Cyber Defense education. We are a Department of Defense Center of Excellence in Cybersecurity Research and we are a Department of Energy cybersecurity consortium leader for workforce development.

This (unintelligible) NSU has won 18 major cybersecurity grants and contracts totaling $43 million. Most awards are from the Department of Energy including the prestigious $25 million consortium enabling cybersecurity opportunities and research and $5 million to establish the Center of Excellence Cybersecurity Research from DoD. This is a very prestigious award as NSU is the only school selected in this effort that does not offer a PhD in computer science. Next slide, please.

The CECOR project leverages the strength of historically black colleges and universities to positively influence the cybersecurity workforce shortage with highly qualified researchers and practitioners. Our consortium consists of 13 colleges and universities, two an energy national laboratory, a K-12 coordinator and a consortium evaluator. Next slide, please.

Our mission is to provide (unintelligible) opportunities to underrepresented students to enhance the cybersecurity workforce. Our goals include building consortia and institutional capacity in cybersecurity to develop and implement

education and training programs for K-20 to conduct cybersecurity related research.

The sponsor workforce development initiative to establish government, corporate and educational partnerships, after that developed a CECOR scholar certificate program to be recognized by industry as providing qualified cybersecurity personnel. Next slide, please.

As shown on the screen, CECOR combines many activities to build capacity and strengthen HBCUs in the very specific disciplines of cybersecurity. Next slide, please.

At the core of our outreach initiative our engaging summer camp set focus on underrepresented populations that partner institutions to include girls in STEM and subsequently women in cybersecurity. Next slide.

Our camps include opportunities for middle school and high school students to learn specific cybersecurity techniques such as forensics, solve the problem, write the documentation and present their findings to give the students an opportunity to exercise and build their soft skills. Next slide, please.

Undergraduate students from CECOR partners and other universities have the option to participate in research experiences for undergraduates on campus and with our national lab partners Lawrence Livermore and Sandia National Laboratories. Next slide, please.

Additionally students have the opportunity to enhance their skill set via camps presentations, focused workshops in Python and Linux and faculty can also participate in externships at the labs as well. Next slide, please.

To date we have had great success. Students, faculty and universities have seen considerable growth toward our goal. Next slide, please. Embedded within NSU's McDemmond Center for Applied Research, our one of a kind 6,000 square foot cybersecurity complex opened in April 2018. Developed in phases the complex offers many interdisciplinary activities that include cyber-psychology, socio-cybersecurity, Cloud computing, big data analysis, and (unintelligible) to perform cyber outreach. Next slide, please.

With the total investment of $4 million, the complex has workstations for 120 students and offices for 16,000 faculty members. We have faculty from computer science, psychology and sociology working together to really cover the broad aspects that are cybersecurity. The end result is the facility that brings Norfolk State cybersecurity efforts under one roof in a pretty unique and exciting way. Next slide, please.

Created with the 2009 CAE designation given our information assurance research education and development institute primarily staffed with computer science faculty and led by Dr. Jonathan Graham, the complex allows us to expand and collocate campus cybersecurity faculty and effort. Students can attend classes, develop virtual machines and work in small groups within cubicles or research efforts. Next slide, please.

The cybersecurity lab that designed as the cyber range allows students to log in and select from multiple virtual machine environments that supports cyber training. The lab also includes a closed network for malware reverse training where students can work with malware in a secured environment and a digital forensics laboratory equipped with the (unintelligible) data center. Both forsenic tools like EnCase and FTK and P2 commander and mobile forensics offering from (unintelligible), Cellebrite, and (unintelligible). Next slide, please.

At the heart of our complex is our Center of Excellence in Cybersecurity Research which features our cyber analysis simulation and experimentation environment or KV led by Dr. Shane. It is a cooperative agreement funded by the Department of Defense between NSU and the Virginia Modeling and Simulation Center at Old Dominion University with objectives to conduct research, perform outreach and be a valued resource for the nation, commonwealth of Virginia, the Hampton roads region and our HBCU minority interest community. Next slide, please.

The research infrastructure includes data that are enterprise graded (unintelligible) with a direct object cyber link to ODU. The data center has multi-functional and modular architecture with Cloud computing and big data platform with substantial capacity for a current and future need. Next slide, please.

We have recently acquired new infrastructure to build an efficient collaborative enterprise governance risk and compliance program across IT finance operations and legal domain. These solutions include policy risk, compliance, enterprise incident vendor threat, business continuity and audit management. This gives us another hands on environment where graduate students can actively engage in policy risk and audit management research on production grade equipment which I believe is the natural extension to complement the existing resources available within the cybersecurity complex.

We will also develop an office (unintelligble) contributions from the private sector. The complex will offer professional development courses made by industry representatives and can award certificates of completion and badges. Students electing to participate will be assigned viable work assignments to

support their interest in academic program. Additionally, we will participate in the exploration of the development of a cyber-security contracting hub. Next slide.

NSU has a unique history of supporting our nation's cybersecurity mission by leveraging faculty, student skills to provide real-time innovative cyber solutions and highly skilled personnel. NSU merits and consequently seeks special designation by the Department of Defense as a provider of cybersecurity services. As we look toward the future our goal is to leverage our work as the leader among HBCUs to navigate new opportunities to diversify innovation and income for historically black colleges and universities. Next slide.

Thanks for the opportunity to share. I am Dr. Aurelia Williams. Please feel free to contact me as needed. Thank you.

Bruce Berger: Thank you Dr. Williams for an exquisite oral compendium of Norfolk State University's capabilities and the value proposition that they have for the cybersecurity space. And we've only got about 5 minutes left so I'm turn it back over to Francine for Q&A.

Francine Alkisswani: Thank you, thank you, all of you. We will now begin the Q&A portion of the webinar. So if you haven't already done so ask you -audience, participants to please type your questions or comments into the question box on the right hand side of the screen.

And I will start this with the first question I guess of how -and this goes to any one of you or all of you. How did you get or how did you see the use of broadband or get your university to invest in broadband or the enabling

infrastructure -cyber infrastructure for the resources to carry out your cybersecurity program? Do you want to start Dr. Williams?

Aurelia Williams: As I mentioned at Norfolk State University we had a couple of staff and active faculty members who were students. I was one of them who was graduated and gone to work for the NSA who came back, who were introduced to cyber at that location and came back and introduced it to the university and the Computer Science department.

Subsequently, we applied –created forces applied for the CAE designation. Once we received that designation a lot of opportunities for grants and external funding became available. So for NSU we actually acquired about $42 million before we had the university to invest the $4 million that was shared. So we had a proof of concept that worked out really well. We had a lot of federal support and therefore the university through our presidential priority ultimately provided additional resources for us to combine in the complex.

Francine Alkisswani: Okay thank you. Someone has asked either any initiative to hire minority professors for your cybersecurity programs. Dr. Kornegay?

Dr. Kornegay: Yes we're actually going through a search right now which is soon to close but if they're interested they can visit the university website and go to 'select the employment opportunity' section of the website and they can see the CAP center positions listed there.

Francine Alkisswani: Another question is did -for each of the presenters and it's interesting what do you need from us in the audience to help you succeed? Who would like to go first on that and we only have about a minute or two to wind this up.

Dr. Kornegay: So I would say when this presentation is repeated where it gets posted, review the presentation. Make sure you get our contact information. I know from experience everyone on this panel is open and willing to collaborate.

Francine Alkisswani: Thank you, Karl. I want to get to one more question here. Someone says, "I run a program for middle and high school students who are studying computer science. Would your initiative be able to provide any curriculum for us to include cybersecurity training?" Dr. Williams? Who would like to go there?

Aurelia Williams: Sure. We have a number of modules that we created. Actually we host a middle school and high school summer camp every year and we have modules who work with Norfolk Public Schools. So those things we would definitely be willing to share if you just contact us to let us know if you're interested.

Francine Alkisswani: And the final comment here is can other HBCUs join the consortium and how. And my suggestion would be to pay attention to the contact information that has been provided or would be provided for you. Now I think I'm going - I'm sorry but that's all the time we're going to have for questions.

Thank you for all the great questions. Unfortunately that is all the time we have; so we hope you can join us again on May 15 for our next webinar entitled, *Infrastructure Week Leveraging Public Assets to Accelerate Broadband Deployment*. Thank you again to our speakers and to everyone who joined the webinar. So as a reminder the presentation, transcript and audio recording will be available on the BroadbandUSA website within seven days.

Finally BroadbandUSA is available for technical assistance to expand broadband connectivity and to promote digital inclusion in broadband

adoption. So for more information please email BroadbandUSA at ntia.gov or visit our Web site for more information and to access our tools and publications. Thank you, thank you all. Thank you panelists, thank you to attendees. Thank you all and have a wonderful afternoon everyone.

END