HBCU Model Programs and Practices for Building a Competitive Cybersecurity Workforce

NTIA Webinar Series

Dial in to listen to the webinar
Conference Line: 800-593-7190 Passcode: 984-4951#

April 17, 2019
Participants

Presenters

• Karl Cureton, Executive Chairman, National Minority Technology Council and Executive Director, Minority Cyber Inclusion Council
• Dr. Kevin T. Kornegay, Professor and IoT Security Endowed Chair, Director of Cybersecurity Assurance and Policy (CAP) Center, and Director, Center for Reverse Engineering and Assured Microelectronics (CREAM), Morgan State University
• Dr. Aurelia T. Williams, Executive Director of the Cybersecurity Complex and Lead PI for the Consortium Enabling Cybersecurity Opportunities and Research (CECOR), Norfolk State University

Moderators

• Francine Alkisswani, Telecommunications Policy Analyst, NTIA, Department of Commerce
• Dr. Bruce Berger, JD, MBA, Lead, HBCU Cybersecurity Cluster & Director, Center for Innovation and Entrepreneurial Development, Clark Atlanta University
Helpful Information

Questions
• Please type questions and comments in the question box on the right hand side of the screen. Questions will be taken after the final presenter.

Presentation
• The presentation along with a transcript and an audio recording will be available on the BroadbandUSA website within 7 days of this webinar under Events/past events.
• https://broadbandusa.ntia.doc.gov/past-event

Technical Assistance
• Guides, products, publications, and other tools are available to assist you with the planning, funding and implementation of your broadband project.
• https://broadbandusa.ntia.doc.gov

*To listen to the webinar: Conference Line: 800-593-7190 Passcode: 984-4951#
Historically Black Colleges and Universities

HBCUs
Stronger Together – Consortia Building

Dedicated to Serving the Underserved – Need for Capacity Building & Infrastructure

National Strategic Asset

Excellence in Cybersecurity, getting Workforce ready

Economic Ecosystem
Anchor Institutions – 5G, Opportunity Zones, Research Innovation

Dr. Bruce Berger, JD, MBA - Moderator
- Lead, HBCU Cybersecurity Cluster
- Director, Center for Innovation and Entrepreneurial Development, Clark Atlanta University
Presentations

• Karl Cureton, Executive Chairman, National Minority Technology Council and Executive Director, Minority Cyber Inclusion Council

• Dr. Kevin T. Kornegay, Professor and IoT Security Endowed Chair, Director of Cybersecurity Assurance and Policy (CAP) Center, and Director, Center for Reverse Engineering and Assured Microelectronics (CREAM), Morgan State University

• Aurelia T. Williams, Executive Director of the Cybersecurity Complex and Lead PI for the Consortium Enabling Cybersecurity Opportunities and Research (CECOR), Norfolk State University
Model Programs and Practices for Building a Competitive Cybersecurity Workforce

Cybersecurity Workforce

Industry Association Sponsored Research

HBCU Student/Faculty Engagement

National Minority Technology Council
Looking Forward Research & Development
Karl Cureton, Managing Director
Minority Cyber Inclusion Council
Chairman Emeritus
National Minority Technology Council
Co-Principal Investigator
Looking Forward Research & Development

20 Years of Service
International Trade Association

Council Exchange Board of Trade
National Minority Technology Council

- 501c6 Business League
- 65,000 Minority Technology Employers
- Minority Tech Employer Firms Earn $100 Billion in Total Combined Annual Sales
- Minority Tech Employers provide over 500,000 Jobs worldwide
- One of our Nation’s Fastest Growing Industries
- NMTC is a Federal Innovation Stakeholder Partner
- National Opportunity Fund Administrator, Investing in Communities and Qualified Opportunity Zone Businesses
Stakeholder Mission Alignment

- Increase Applied Research
- Increase Contract Funding
- Increase Interoperability
- Increase # Jobs & Salaries
- Increase Outcome Metrics

Understanding the Governance of Innovation and Community-Oriented Outcomes

Creating Tech-Based Economic Development Ecosystems

Looking Forward Research & Development

20 Regions – 40 Districts
Industry Partnerships = University Opportunities

HBCU Research & Innovation on convergence between 5G and Cybersecurity

- University Led Broadband Investments bring Community Economic Development
- Both Faculty & Student Enrichment from Applied Research & Innovation
- Regional Alliance Partnerships with Industry Needed in HBCU community
- Interdisciplinary Cybersecurity Curriculum Development for Relevant Employer Career Paths
HBCU Consortia Building

www.outcomefund.us

- Industry Association focused on jobs and creating new learning opportunities – research & building systems to help get our communities workforce ready

- HBCUs are Anchor Institutions for Economic Development and are located in Opportunity Zones

- HBCUs serve a U.S. population prime for a historical increase in social economic empowerment and growth in wealth, ready in capability, resilience with scalable human potential.
Cybersecurity & the Internet Economy

• Promote Innovation and Emerging Technologies
• Advocate for Minority Inclusion in the Cybersecurity Workforce
• Research, Program & Deploy an Industry focused Cybersecurity Workforce Certification Program
• Strategically connect Minority Students to Employers and Industry Use Cases

Minority Cyber Inclusion Council

www.mcicouncil.org
Historically Black Colleges and Universities (HBCUs) are a critical national resource. Jointly assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education.
Cybersecurity Workforce in Context

U.S. Public & Private Sector Crisis

- Federal Government Estimates +300,000 active openings for U.S. Cybersecurity Related Jobs
- 2022 Cybersecurity Demand +1.8 Million Jobs
- Minorities and Women are Underrepresented in Cybersecurity Workforce
- **Pay for Cybersecurity Jobs are above average** (Public Sector Challenge – Reform Proposal CTMS)
- Employers Concerned with Cybersecurity Related Education – Teacher Shortage is a Challenge
- Adjudication for Security Clearance is a Challenge
- Orientation best started at Middle School
Private & Public Sectors need to align education and training with employers’ cybersecurity workforce needs.
124,389 Analyze  
+ 88,175 Oversight & Dev.  
212,564 MCI Council Focus

### Cybersecurity Workforce Framework

#### Job Openings by Nice Cybersecurity Workforce Framework Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Openings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operate &amp; Maintain</td>
<td>207,190</td>
</tr>
<tr>
<td>Securely Provision</td>
<td>186,864</td>
</tr>
<tr>
<td>Protect &amp; Defend</td>
<td>129,716</td>
</tr>
<tr>
<td>Analyze</td>
<td>124,389</td>
</tr>
<tr>
<td>Collect &amp; Operate</td>
<td>49,825</td>
</tr>
<tr>
<td>Oversee &amp; Govern</td>
<td>88,175</td>
</tr>
</tbody>
</table>

Note: The Investigate category usually has fewer openings than other categories and may not be visible in the chart. To view data for the Investigate category, please hover over the thin line in the bottom right of the visualization.
Building on and strengthening hands-on, experiential and work-based learning approaches—including apprenticeships, research experiences, co-op programs and internships

Transform, Elevate, and Sustain the Learning Environment to grow a Dynamic and Diverse U.S. Cybersecurity Workforce

www.hbcucompete.org
www.uasnavigator.org
www.tech-africa.org

MCI
Minority Cyber Inclusion Council

nmtc
LOOKING FORWARD
Next Steps & Thank You

Council@NMTCImpact.org
www.nmtcimpact.org
www.mcicouncil.org

National Minority Technology Council
Presentations

• Karl Cureton, Executive Chairman, National Minority Technology Council and Executive Director, Minority Cyber Inclusion Council

• Dr. Kevin T. Kornegay, Professor and IoT Security Endowed Chair, Director of Cybersecurity Assurance and Policy (CAP) Center, and Director, Center for Reverse Engineering and Assured Microelectronics (CREAM), Morgan State University

• Aurelia T. Williams, Executive Director of the Cybersecurity Complex and Lead PI for the Consortium Enabling Cybersecurity Opportunities and Research (CECOR), Norfolk State University
Cybersecurity Assurance and Policy Center
“The CAP Center”

Dr. Kevin Kornegay
IoT Security Chaired Professor & Director
(443) 885-4869
kevin.kornegay@morgan.edu
www.iotcream.com
5G Technology

- Mobile broadband
- Dense crowd of users
- Very high data rate
- Mobility
- Very high capacity
- Massive number of devices
- Reliability, resilience, security
- Long battery lifetime
- Very low latency
- IoT sensor network
- IoT control network
Are you ready?

Ubiquitous Connectivity Among People and Devices

- Broadband Wireless Internet Access
- Sensor Networks
- Smart Homes/Spaces
- Automated Highways
- Smart Grid
- Body-Area Networks
- Internet of Things
- All this and more…

Center for Reverse Engineering and Assured Microelectronics
CAP Center

• What is the CAP Center?

Impact
• SME’s
• CD Education
• Economy
• Workforce
• Sustainable
• Vision
  o To become the 1st HBCU CAE-R

• Mission:
  o Provide intelligence community with knowledge, methodology, solutions, and highly skilled cybersecurity professionals to prevent penetration and manipulation of our nation’s cyber physical infrastructure.

• Research Objectives:
  o Conduct physical layer cybersecurity research using invasive and noninvasive hardware/software reverse engineering techniques to assess the assurance of IoT systems.
  o Conduct Security and privacy policy research
SENSE + PROCESS + TRANSMIT = IoT Device

Research: IoT Device Hardware Assurance

No. of IoT Devices

IoT Device Vulnerabilities

An **unintended** channel for monitoring or operating a device resulting from its physical interface.

**Intended**
- Keypad
- Screen
- Card Reader
- Speaker
- USB
- Bluetooth/WiFi
- Power

**Unintended**
- Power Consumption
- EM Radiation
- Sound
- Temperature
- Time
- Light

In relation to a security operation, a side channel can lead to a compromised system!
CAP Faculty

Dr. Kevin Kornegay
HW Assurance

Dr. Michel Reece
Wireless Authentication

Dr. Willie Thompson
Software Defined Radio

Dr. Kofi Nyarko
Data Analytics

Dr. Kemi Ladeji-Osias
Engineering Education/Outreach
Education: Secure Embedded Systems Graduate Curriculum

Design
- Secure Embedded System Design
- Advanced Digital System Design
- Embedded Software Design
- System-on-a-Chip FPGA Design
- Machine Learning
- Operating Systems
- Programming Languages
- AI/Machine Learning

Embedded Systems
- Cryptography
- Intro to Network Security
- Hardware Reverse Engineering
- Advanced Secure Embedded Systems
- Cyber Physical System Security
- Digital Forensics Technologies and Techniques

Communications
- RF Communication Systems
- Digital Communications
- Communication Networks
- Protocol Design
- Microwave Systems and Components
- Active Microwave Circuit Design
- Intro to Microwaves

Note: Some courses are offered by JHU via MSU/JHU Memo of understanding
CREAM Cyber Scholar Skills Profile

**CREAM Cyber Scholar**

**Cryptography**
- Asymmetric Encryption
- Symmetric Encryption
- Message Authentication Codes

**Communications**
- Wireless/wired networks
- Protocols and standards

**Software**
- Operating Systems
- Virtual Machines
- Programming Languages
- AI/Machine Learning
- Reverse Engineering

**Hardware Assurance**
- System-on-Chip (SoC)
- Trusted Platform Modules
- Software Defined Radio
- Software Defined Networks
- Reverse Engineering
CAP Scholars

• 13 DEN Students
  o 5 Women (40%)
  o 8 African American (70%)
  o 1\textsuperscript{st} DEN graduated in Dec 2018, currently CAP Postdoc
  o Most of the students are at least in their 3\textsuperscript{rd} year of study

• Prestigious Graduate Fellowships
  o 2 DoD/NSA CySP Scholarship Recipients
  o 5 GEM Doctoral Fellowships (3 Full, 2 Associate)

• 25+ Undergraduate Student Researchers
Degree Programs & Certifications

- Bachelor of Science in Electrical Engineering with Cybersecurity Track
- Master of Engineering in Cyber Engineering (Professional)
- Doctor of Engineering in Embedded Systems
- Future
- Bachelor of Science in Computer Science Cybersecurity Track
- Bachelor of Science in Information Systems Cybersecurity Track
- Master of Science in Cyber Security
- Master of Science in Information Systems Cybersecurity
- Doctorate of Engineering in Hardware Security (Proposed New Program)
Thank You &
Contact Information

Dr. Kevin Kornegay
IoT Security Chaired Professor & Director
(443) 885-4869
kevin.kornegay@morgan.edu
www.iotcream.com
# Presentations

- **Karl Cureton**, Executive Chairman, National Minority Technology Council and Executive Director, Minority Cyber Inclusion Council

- **Dr. Kevin T. Kornegay**, Professor and IoT Security Endowed Chair, Director of Cybersecurity Assurance and Policy (CAP) Center, and Director, Center for Reverse Engineering and Assured Microelectronics (CREAM), Morgan State University

- **Aurelia T. Williams**, Executive Director of the Cybersecurity Complex and Lead PI for the Consortium Enabling Cybersecurity Opportunities and Research (CECOR), Norfolk State University
NSU Cybersecurity History

• Cybersecurity Educational Pathways
• Capabilities
  • Partnerships and Collaborations
  • Awarded Grants and Contracts
  • Facilities: Laboratories, Hardware, and Software
• Outreach
NSU Cybersecurity Capabilities

Partnerships and Collaborations
• NSA/DHS Center of Academic Excellence in Cyber Defense Education
• DOD Center of Excellence in Cybersecurity (Research)
• DOE Cybersecurity Consortium Leader for Workforce Development

Awarded Grants and Contracts
• Since 2010, NSU has won 18 major cybersecurity grants and contracts totaling $43M
• Most awards are from the Department of Energy, including the prestigious $25M “Consortium Enabling Cybersecurity Opportunities and Research” and $5M “Center of Excellence in Cybersecurity (Research)” from DoD.
Consortium Enabling Cybersecurity Opportunities and Research

Consortium Partners

- Allen University
- Benedict College
- Bowie State University
- Claflin University
- Clark Atlanta University
- Denmark Technical College
- Lawrence Livermore National Laboratory
- Morris College
- \textit{Norfolk State University} – \textit{Lead University}
- North Carolina A&T State University
- Paine College
- Sandia National Laboratories
- South Carolina State University
- University of the Virgin Islands
- Voorhees College
Consortium Enabling Cybersecurity Opportunities and Research

Vision
To become recognized as a leader in developing highly-qualified cyber security researchers and practitioners reflective of the US population demographics.

Mission
Establish a consortium of educators, students, and professionals to provide STEM opportunities to underrepresented students to enhance the cyber security workforce.

Goals
- Build consortium and institutional capacity in cybersecurity
- Develop and implement education and training programs for K-20
- Conduct cybersecurity related research
- Sponsor workforce development initiatives
- Establish government, corporate, and educational partnerships
- Develop the CECOR Scholar Certificate Program to be recognized by the industry as providing qualified cybersecurity workforce.
## Consortium Activities

<table>
<thead>
<tr>
<th>Cybersecurity Capacity Building</th>
<th>Education and Training</th>
<th>Research</th>
<th>Workforce Development</th>
<th>Partnerships</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment acquisitions and upgrades</td>
<td>Middle and high school cybersecurity summer camps</td>
<td>Academic year research</td>
<td>Summer teacher training in cybersecurity for middle and high school teachers</td>
<td>DOE laboratories provide guidance in curriculum development</td>
</tr>
<tr>
<td>Software acquisitions and upgrades</td>
<td>MOU and articulation agreements between CAE institutions and consortium members</td>
<td>Student research experiences at CAE Institutions</td>
<td>Faculty development hosted by CAE universities</td>
<td>CAE universities provide guidance in curriculum development</td>
</tr>
<tr>
<td>Infrastructure enhancements to include the establishment of a teaching lab in SC</td>
<td>Tracer Fire cybersecurity Boot Camps for consortium students</td>
<td>Student internships with industry partners</td>
<td>Faculty research internships at DOE laboratories</td>
<td>Industry partners host students for summer experiences</td>
</tr>
<tr>
<td>Scholarship support for undergraduate students enrolled in cybersecurity concentrations</td>
<td>Pre-college institute for incoming freshmen</td>
<td>Faculty research internships at DOE laboratories</td>
<td>Academic year training in computer science for middle and high school teachers</td>
<td>Development of federal and corporate K-20 partnerships</td>
</tr>
<tr>
<td>Scholarship support for graduate students enrolled in cybersecurity concentrations</td>
<td>Cybersecurity course and curriculum design, development, deployment and enhancement</td>
<td>Faculty research at local campuses and mentoring students in cybersecurity related areas</td>
<td>Student internships at DOE laboratories and SPAWAR</td>
<td></td>
</tr>
<tr>
<td>New faculty and staff hires</td>
<td>Boot Camp for LLNL bound students</td>
<td>Mobile applications development with high school students in CCSD</td>
<td>K-12 outreach and pipeline development</td>
<td></td>
</tr>
<tr>
<td>Resource and Information sharing across the consortium</td>
<td>Boot Camp for SNL bound students</td>
<td></td>
<td>Development and implementation of training programs</td>
<td></td>
</tr>
<tr>
<td>Faculty lab start-up packages</td>
<td>STEM curriculum development at CCSD</td>
<td></td>
<td>Advice on K-12 STEM development and activities</td>
<td></td>
</tr>
<tr>
<td>DOE labs provide technical guidance to the consortium and its governing board</td>
<td>Implementation of 3D programming to CCSD students</td>
<td></td>
<td>Outreach and awareness to CGSD and 2-year colleges from consortium members</td>
<td></td>
</tr>
<tr>
<td>Development of K-12 cybersecurity modules</td>
<td></td>
<td></td>
<td>Academic year internships</td>
<td></td>
</tr>
</tbody>
</table>
**K-12 Summer Camps**

---

**STEM Girls Rock! & My Brother’s Keeper**

In partnership with SPAWAR,

- 100 rising 8th and 9th grade female students and a parent were exposed to Science, Technology, Engineering and Math (STEM) related degrees and career opportunities in a fun and interactive way.

In partnership with LLNL,

- Bay Area students were exposed to the “My Brother’s Keeper” initiative launched by President Obama.
Cyber Security Summer Academy

- High School Students learn the basics of computer forensics, cyber security and solve a case using forensics techniques learned during the camp
Research Experiences for Undergraduates

NSU Summer Internships

Fig. 1: Elinado DelRosario and Gabriel Ramos presented their summer research completed at NSU during the Fall Undergraduate Research Symposium, UNF
Camps, Competitions, Conferences

Python Bootcamp, NSU

Undergraduate Research Symposium, UVI

Presentations to Businesses, UVI

Debate legal, policy and technical topics

LEGO® Pi – build it and program it

Claflin Faculty, Deidra Morrison at LLNL for 12 weeks
CECOR Consortium Success

• Build consortium and institutional capacity in cybersecurity.
  - 10 new labs @ 8 Schools
  - 61 faculty trained in Cybersecurity
• Develop and implement education and training programs for K13-20.
  - 8 new programs @ 6 schools;
  - 88 new/improved courses @ 11 schools
  - 237 BS, 91 MS, and 4 PhD degrees
• Conduct cybersecurity related research.
  - 35 publications @ 7 partners;
  - 251 students participated in active research
• Sponsor workforce development initiative.
  - 2417 students participated in Cybersecurity Summer Camps
  - 224 graduated entered the workforce; 32 with cybersecurity-related titles
• Establish government, corporate, and educational partnerships.
  - Numerous partnerships have been established due to this important work
NSU Cybersecurity Complex

- Total Investment: $4M
  – With $1M from DOD HBCU/MI Program
- Secure: Isolated from NSU network
- Offices, conferencing area, office equipment
Complex Centers and Laboratories

Information Assurance Research, Education, and Development Institute (IA-REDI)
Complex Centers and Laboratories

- Digital and Mobile Forensics Laboratory
- Capture the Flag and Networking Teaching Environment
- Malware Reverse Engineering Laboratory
- Cybersecurity Training
Center Of Excellence Cybersecurity Research

Cooperative Agreement Funded by Department of Defense
• Lead Institution: Norfolk State University (Computer Science; IA-REDI)
• Collaborator: Old Dominion University (VMASC)

Objectives
• Conduct basic research
  − To develop a cloud-enabled, big-data-analytics-capable Cyber Analysis, Simulation and Experimentation Environment (CASE-V)
  − For enhancing situational awareness and decision support for cyber defense and cyber training
  − Focusing on advanced persistent threat (APT)
• Perform research-related education and outreach activities
• Be a valued resource
  − For the Nation, Commonwealth of Virginia, Hampton Roads Region, and HBCU/MI Community
  − In cybersecurity research, education, outreach, and workforce development
COE Research Infrastructure & Datacenter

- Direct optic fiber link between NSU and ODU (new): City of Norfolk
- ODU Cloud Research and Cybersecurity Research Labs (new)

- State-of-the-art enterprise-grade equipment
- Multi-functional & modular architecture
- Substantial capacity
  - Hard disk storage: ~820 Terabytes
  - Server-grade CPU cores: ~1,700
  - Main memory: ~7.5 Terabytes
  - 10/40 Gbps LAN connectivity
Cybersecurity Complex

New Activities

- Infrastructure acquisition to offer a research environment for students to engage in policy, risk, and audit management research on production grade equipment.
- Launch a professional development office to offer certifications in enterprise governance, risk and compliance (eGRC).
- Investigate the design of a framework to leverage existing infrastructure into the development of a Cybersecurity contracting hub.
NSU Cybersecurity Educational Strengths Summary

• Designated **NSA/DHS Center of Academic Excellence in Cyber Defense Education** through 2020
• Extensive online cybersecurity laboratories and facilities and the capability of delivering programs worldwide
• Collaborations with national laboratories and other government agencies
• Well-qualified faculty
• Significant external funding
• Innovative ideas to lead the HBCU community
Additional Information

Dr. Aurelia T. Williams
Executive Director, Cybersecurity Complex
Professor, Computer Science Department
Norfolk State University

E-mail: cybersecurity@nsu.edu
Telephone: (757) 823-9454
Facsimile: (757) 823-9229
Web: www.nsu.edu
HBCU Model Programs and Practices for Building a Competitive Cybersecurity Workforce

Questions and Comments

• Please type your questions in the question box.

• The slides, transcript, and an audio recording will be posted on the BroadbandUSA website within 7 days of the webinar.

https://broadbandusa.ntia.doc.gov/past-event
Thank you for attending.
Tune in for the next Practical Conversations Webinar

Infrastructure Week: Leveraging Public Assets to Accelerate Broadband Deployment

May 15, 2019
2:00 pm EST

Registration is required for each webinar:
https://broadbandusa.ntia.doc.gov/event
BroadbandUSA is available to help communities with their broadband access and digital inclusion efforts

For General Information:

202-482-2048
broadbandusa@ntia.gov
https://broadbandusa.ntia.doc.gov/resources

To Request Technical Assistance (TA):

Broadband TA Request Form -
https://broadbandusa.ntia.doc.gov/ntia-common-content/how-we-can-help

BBUSA Resources

- Implementing a Broadband Network Vision: A Toolkit for Local and Tribal Governments
- Community Broadband Roadmap Toolkit
- Guide to Federal Funding of Broadband Projects
- Using Partnerships to Power Smart Cities