HBCU COMPETITIVENESS:
Aligning Institutional Missions With America’s Priorities

2018 NATIONAL HISTORICALLY BLACK COLLEGES AND UNIVERSITIES WEEK CONFERENCE

September 16-19, 2018
Washington Marriott Wardman Park
2660 Woodley Road, NW
Washington, DC 20008
Smart HBCUs Building the Cybersecurity Workforce

Facilitator: Bruce Berger, Executive Director, Center for Innovation and Entrepreneurial Development, Clark Atlanta University

Panelists: Karl Cureton, Executive Chairman, National Minority Technology Council/Minority Cyber Inclusion Council

Kevin T. Kornegay, Professor and IoT Security Endowed Chair, Morgan State University

Aurelia Williams, Director Cybersecurity Complex, Norfolk State University
Smart HBCUs Building the Cybersecurity Workforce

• Smart HBCUs are resilient--dedicated to helping HBCU communities around the Nation become more resilient to the physical, social and economic challenges that are a growing part of the 21st century.

• Smart HBCUs are transformative--have the potential to foster stronger financial cooperation between the private and public sectors, create processing efficiencies, and increase innovation for service-related infrastructural projects.

• Smart HBCUs are a platform to collaborate with the private sector to source innovative financing, leverage technical expertise and push forward-leaning projects to the starting line.

• Smart HBCUs are a platform for inclusive competitiveness and for aligning institutional mission with America’s priorities.
Cybersecurity Assurance and Policy (CAP) Center

Dr. Kevin Kornegay
IoT Security Professor & Director
Morgan State University
Baltimore, Maryland
Cybersecurity Assurance and Policy (CAP) Center

Dr. Kevin Kornegay
IoT Security Professor & Director
Morgan State University
Baltimore, Maryland
What is the CAP Center?

Education
NSA/DHS
CAE-CD

Research
NSA/DHS
CAE-R

Impact
• Experts
• CD Education
• Economy
• Workforce
• Sustainability

White House Initiative on Historically Black Colleges and Universities
CAP Center

• Vision
  – To become the 1st HBCU CAE-R

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

• Research Objectives:
  – Conduct physical layer cybersecurity research using invasive and noninvasive hardware/software reverse engineering techniques to assess the assurance of IoT systems.
  – Conduct Security and privacy policy research
<table>
<thead>
<tr>
<th>University</th>
<th>Core Areas (7)</th>
<th>Infrastructure</th>
<th>Unclassified/Classified</th>
<th>Carnegie Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>JHU</td>
<td>2</td>
<td>APL</td>
<td>Both</td>
<td>R1</td>
</tr>
<tr>
<td>UMBC</td>
<td>4</td>
<td>Lockheed Martin, Northrop Grumman</td>
<td>Both</td>
<td>R2</td>
</tr>
<tr>
<td>UMCP</td>
<td>7</td>
<td>LTS, LPS, IARPA, UMUC</td>
<td>Both</td>
<td>R1</td>
</tr>
<tr>
<td>Morgan</td>
<td>2</td>
<td>McMenemy Hall 5th Floor</td>
<td>Unclassified</td>
<td>R3</td>
</tr>
</tbody>
</table>
Research: IoT Device Assurance

SENSE + PROCESS + TRANSMIT = IoT Device

CAP Team

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
Partners and Sponsors

NSF
NATIONAL SECURITY AGENCY
APL
JOHNS HOPKINS APPLIED PHYSICS LABORATORY
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LOCKHEED MARTIN
XILINX®
MIT
JOHNS HOPKINS WHITING SCHOOL OF ENGINEERING
Information Security Institute
MARYLAND
Dartmouth
VT
VIRGINIA TECH
CAPITOL TECHNOLOGY UNIVERSITY
## Research Funding

<table>
<thead>
<tr>
<th>Agency</th>
<th>Award Year (Start-End)</th>
<th>Project Title</th>
<th>Role/Type</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Army</td>
<td>10/2014</td>
<td>Embedded Mobile Tactical Systems -- Reverse Engineering and Countermeasures (Equipment Grant)</td>
<td>PI</td>
<td>$212,000</td>
</tr>
<tr>
<td>Army Research Laboratory</td>
<td>9/25/2015 – 9/24/2020</td>
<td>IDIQ Contract: Design Techniques for Low Power Highly Linear CMOS Transceivers</td>
<td>PI</td>
<td>$3,099,906</td>
</tr>
<tr>
<td>IARPA</td>
<td>10/1/2016-9/30/2021</td>
<td>RAVEN: Nanoscale X-ray Tomosynthesis for Rapid Assessment of IC Dies (MIT Lead)</td>
<td>Co-PI</td>
<td>$12,000,000</td>
</tr>
<tr>
<td>DoD/NSA</td>
<td>5/1/2017-8/31/2017</td>
<td>NSA-LTS/Morgan State University Summer Cyber and Telecommunications Research</td>
<td>PI</td>
<td>$100,000</td>
</tr>
<tr>
<td>DoD/NSA</td>
<td>9/24/2017-9/23/2018</td>
<td>DoD Information Assurance Scholarship Program (IASP): CREAM Scholars and Capacity Building</td>
<td>PI</td>
<td>$212,636</td>
</tr>
<tr>
<td>NSF/CNS: Secure and Trustworthy Cyberspace</td>
<td>Pending Finalist Reverse Site Visit on 3/26</td>
<td>“Securing the Life-Cycle of IoT Consumer Electronics (SLICE)” in collaboration with Dartmouth (Lead), JHU, UMD, and Illinois</td>
<td>Co-PI</td>
<td>$10,000,000</td>
</tr>
<tr>
<td>NSF/HRD</td>
<td>Pending</td>
<td>CREST: Center for Reverse Engineering and Assured Microelectronics (CREAM) in collaboration with CS, CE, ECE, Transportation, JHU, Applied Physics Lab, and VaTech</td>
<td>PI</td>
<td>$5,000,000</td>
</tr>
<tr>
<td>DoD/NSA</td>
<td>Pending</td>
<td>DoD IASP: CREAM Scholars and Capacity Building II</td>
<td>PI</td>
<td>$407,156</td>
</tr>
</tbody>
</table>
Education: Secure Embedded Systems Graduate Curriculum

- Secure Embedded System Design
- Advanced Digital System Design
- Physical Layer Hardware Design
- Embedded Software Design
- System -on-a-Chip FPGA Design
- Machine Learning

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

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/CREAM Scholars

- 12 DEN Students
  - 4 Women (33%)
  - 9 African American (75%)
  - 1st Doctorate in fall 2018
  - Most of the students are at least in their 3rd year of study
- Prestigious Graduate Fellowships
  - 2 DoD/NSA IASP Scholarship Recipient
  - 5 GEM Doctoral Fellowships (2 Full, 3 Associate)
- 20 Undergraduate Student Researchers
- 3 Refereed Technical Conference Papers
- 1 US Patent
Faculty Clusters

• IoT Security Cluster (Hire 5 Faculty in AY 2019)
  – SCMNS: Light-Weight Cryptography
  – SOE/ECE: Software Reverse Engineering, Digital Forensics, AI & Embedded Systems
  – Business: Security or Privacy Policy

• Cyberwar and Critical Infrastructure (Hire 3 Faculty in AY 2020)
  – TBD
NSU Cybersecurity Complex

Dr. Aurelia T. Williams, Executive Director
NSU Cybersecurity History

• Cybersecurity Educational Pathways
• Capabilities
  - Partnerships and Collaborations
  - Awarded Grants and Contracts
  - Facilities: Laboratories, Hardware, and Software
• Outreach
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)
- Digital and Mobile Forensics Laboratory
- Capture the Flag and Networking Teaching Environment
- Malware Reverse Engineering Laboratory
- Cybersecurity Training
- SocioCybersecurity
- Cyber Outreach
- COE Datacenter & Cybersecurity Research Lab
- Cyberpsychology Lab
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 Research, Education and Development Institute (IA-REDI)
- Collaborator: Old Dominion University
  - Virginia Modeling, Analysis and Simulation Center (VMASC)
COE Research Program

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

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

- State-of-the-art enterprise-grade equipment
- Multi-functional & modular architecture
  - Cloud computing platforms
  - Big data platforms
  - Shared storage
  - High-performance networks
- Substantial capacity
  - Hard disk storage: ~820 Terabytes
  - Server-grade CPU cores: ~1,700
  - Main memory: ~7.5 Terabytes
  - 10/40 Gbps LAN connectivity
- Installation & operation by COE students and faculty in coordination with NSU IT
Consortium Enabling Cybersecurity Opportunities and Research

Dr. Aurelia T. Williams, Lead PI
Who Are We?

• A collaborative effort funded by the Department of Energy to develop a K-20 pipeline for the workforce; the project will pilot a workforce development program to produce well-qualified cybersecurity professionals in significant numbers to address the pressing cybersecurity workforce shortage

• Partners include HBCUs and national laboratories.
  – 13 HBCUs (4 CAEs) 1 Two-year Technical College
  – Lawrence Livermore National Laboratory, Sandia National Laboratory
Partners

White House Initiative on Historically Black Colleges and Universities
Goal and Objectives

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

Goal
Establish a world-class workforce development, education and research program that combines the strengths of Historically Black Colleges and Universities (HBCUs) and national laboratories to create a K-20 pipeline of students to participate in cybersecurity and related fields.

Objectives
• 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 &amp; 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 externships 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 externships 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>Development and implementation of training programs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Faculty lab start-up packages</td>
<td>STEM curriculum development at CCSD</td>
<td>Advice on K-12 STEM development and activities</td>
<td></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>Outreach and awareness to CCSD and 2-year colleges from consortium members</td>
<td></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>

---

White House Initiative on Historically Black Colleges and Universities
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
K-12 Summer Camps

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.

The Cyber Security Summer Academy

June 27 - July 1, 2016

- Computer Forensics
  Explore techniques universally used to fight cyber criminals

- Cyber Security
  You will learn techniques to protect computer networks and data from attacks and unauthorized access

- Crime Solving
  Solve a computer forensics case using techniques learned in the camp

Contact
Dr. Cheryl Hinds
Computer Science Department
Norfolk State University
700 Park Avenue
Norfolk, Virginia 23504
(757) 823-9551
chinds@nsu.edu

Application Packet
Program Application
Health Form
Teacher Letter of Recommendation
Student Essay

Application Deadline: May 27, 2016

Mail packet to:
Dr. Cheryl Hinds
Norfolk State University
700 Park Avenue, RTC 3201
Norfolk, VA 23504

Fax packet to:
(757) 623-9299

www.nsu.edu

Funded by the Department of Energy
Sponsored by Information Assurance Research, Education and Development Institute (IA-REDI)
Research Experiences for Undergraduates

NSU Summer Internships

White House Initiative on Historically Black Colleges and Universities
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

White House Initiative on Historically Black Colleges and Universities
Evaluation Plan

- Dr. Gwen Lee-Thomas, Quality Metrics, LLC, Consortium Evaluator

**Short Term Metrics**
- Percent or number of new incoming students
- Number of new courses created
- Number of students participating in DOE internship programs
- Retention Rate
- Graduation Rate

**Long Term Metrics**
- Number of Faculty who successfully complete cybersecurity workshop training
- Results of student performance at workshops and internships
- K-20 Cybersecurity Module development and implementation
- Number of graduates
  - with certificates/degrees in cybersecurity
  - placed in a cybersecurity field (advanced degree/workforce)
  - hired into cybersecurity-related employment within the DOE complex
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
Smart HBCUs Building an Inclusive and Competitive Cybersecurity Workforce

Partnerships for Growth - Leveraging Industry Access

*Karl Cureton, Executive Chairman*

*National Minority Technology Council*
Partnerships for Growth - Leveraging Industry Access

Smart HBCUs & Technology Business Owners - Connecting Innovation, Jobs and Broadband
Industry Perspective

- 65,000 Minority Technology Employers
- $100 Billion in Combined Annual Sales
- 500,000 Combined Employees
- 40 Districts across the Nation
- 2025 Goal to reach $1 Trillion in Annual Sales

National Minority Technology Council
Looking Forward Research & Development

Federal Innovation Stakeholder Partner
Tech Industry Minority Outreach & Recruitment

Solving the Industry & Government Cybersecurity Workforce Challenge

• Better alignment with strategic federal investments in education (industry partnerships are key)
• Understanding gaps – Awareness Campaign (PK-20 Cyber Pipeline)
• NIST-NICE Framework
• Cyber Certification (Open Badges) Industry Deployment
• DHS 2019 Change - Cyber Talent Management System (CMTS)
The Why – An Industry Perspective

Capability – Rate - Pipeline
HBCUs Create the people resource

<table>
<thead>
<tr>
<th>LABOR CATEGORY</th>
<th>RATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Engineer II</td>
<td>$132.55</td>
</tr>
<tr>
<td>Cybersecurity Engineer III</td>
<td>$167.56</td>
</tr>
</tbody>
</table>

GSA Schedule

$163.00 * 1,750 hours = $285,250

$285,250 * $185,250 = $100,000 profit

Bachelor’s Degree in computer science, information assurance/security, information science and technology and CISSP-ISSEP or equivalent DoD 8570.01-m IASAE 6 years of relevant experience
Industry Partnerships = University Opportunities

Broadband Attracts High Growth Businesses

• HBCU Innovation = Regional Economic Progress

• Investment in **Time** Generates
  - Money
  - Community Growth
  - Grants
  - Contracts
  - Community Access
Industry Partnerships = University Opportunities

Broadband Attracts High Growth Businesses

- Broadband Investment brings Economic Development
  - Federal, State & Local Funding
  - Private & Social (ESG)
  - Opportunity Zone
    & Opportunity Fund
  - Infrastructure Growth
  - Faculty & Student Capacity
  - Faculty & Student Capability
Smart HBCUs Join the Movement – Be the Change!
Smart HBCUs - Partnerships for Growth

National Minority Technology Council

Karl.Cureton@NMTCouncil.org
202-600-7828

www.nmtcouncil.org

www.mcicouncil.org