

MEMORANDUM OF UNDERSTANDING  
BY AND BETWEEN  
THE UNITED STATES ARMY CYBER CENTER OF EXCELLENCE  
AND  
THE UNIVERSITY OF CENTRAL FLORIDA (UCF) BOARD OF TRUSTEES  
FOR  
COLLABORATION IN PROVIDING  
CYBER RESEARCH, TRAINING AND EDUCATION

(FTG #16-269)

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

This Memorandum of Understanding (MOU) between the USA Cyber CoE and The UCF Board of Trustees (Institution). When referred to collectively, they are referred to as the "Parties".

## 1. BACKGROUND

1.1. As a National Security Agency (NSA) and Department of Homeland Security (DHS) designated National Center of Academic Excellence in Cyber Defense Education (CAE-CDE), UCF is uniquely qualified and well-positioned to support the mission needs of the USA Cyber CoE, located at Fort Gordon, GA. Per the NSA/DHS designation, CAE-CDEs provide the educational programs needed to prepare students for the workforce to protect the National Information Infrastructure. CAE-CDEs must provide depth of education in the following seventeen (17) Knowledge Units (KU):

- Basic Data Analysis
- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- Databases
- Fundamental Security Design Principles
- Information Assurance (IA) Fundamentals
- Intro to Cryptography
- Information Technology (IT) Systems Components
- Network Defense
- Network Technology and Protocols
- Networking Concepts
- Operating Systems Concepts
- Policy, Legal, Ethics, and Compliance
- Probability and Statistics
- Programming
- Systems Administration

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

1.2. CAE-CDEs must have NSA/DHS approved KUs in five (5) additional areas of expertise selected by the institution in accordance with its academic strengths. UCF received the NSA/DHS designation as a CAE for the following six (6) KUs that also directly align with the mission needs of the Cyber CoE:

- Advanced Cryptography
- Advanced Network Technology & Protocols
- Data Structures
- Intrusion Detection / Prevention Systems
- Low Level Programming
- Operating Systems Theory

1.3. UCF, founded in 1963, is the 2nd largest university in the nation and is classified as a Carnegie R1 (Doctoral Universities - Highest Research Activity) institution. Located in Orlando, Florida, UCF's Fall 2015 enrollment was 63,002 including 9,573 students enrolled in the College of Engineering and Computer Science. Fall 2015 records show 1,664 students enrolled in the Bachelor of Science (BS) in Computer Science program and 813 student enrolled in the BS in IT program. The UCF Collegiate Cyber Defense Competition (CCDC) Team, formed in January 2013, won 1st Place in the 2013 Southeast Collegiate Cyber Defense Competition during their inaugural season against teams that had competed consistently for the previous eight (8) years. The UCF CCDC Team twice defended its National Championship title and won the National CCDC's in 2014, 2015, and 2016.

The Institute for Simulation & Training (IST) is an institute of UCF in Orlando, focused on training and simulation related research. A multidisciplinary graduate program leading to a master's and doctoral degree in modeling and simulation is available to students of engineering, computer science, digital media, mathematics, psychology and other related disciplines. Founded in 1982, IST is one of the nation's leading research centers for simulation, training, modeling, virtual, augmented and mixed reality research for both defense and commercial applications. IST employs more than 260 full-time researchers, support personnel and student interns. An aggressive effort to involve students in real-world research has resulted in numerous undergraduate and graduate student research positions. Located in a dynamic, growing field, supported by government and industry sponsors, and charged with identifying new directions for this technology, IST is helping to define the future of simulation and training.

IST's laboratories, workspace and administrative offices occupy more than 80,000 sq. ft. at its three Central Florida Research Park locations, the Partnership II and III buildings and the Simulation Training Technology Center. Large portions of the institute's facilities are configured as laboratories and research workspace. Laboratory space is flexible and reconfigured as projects and programs require. Current laboratories support research in computer generated forces, embedded training, virtual, mixed and augmented reality, computer graphics, high performance parallel processing, interactive

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

entertainment, public safety, advanced distributed learning, computer-controlled robotics, human factors and behavioral science.

These distinct honors and its proximity to Program Executive Office-Simulation, Training and Instrumentation (PEO STRI) and to cyber-related corporate entities in the UCF Research Park in Orlando, FL allows UCF and the IST at UCF to seamlessly facilitate degree and professional development education and training opportunities for the Cyber CoE.

1.4. The USA Cyber CoE is pursuing a long-term, strategic relationship with UCF to access its extensive research, educational, training, and technical resources in support of the Cyber CoE's mission; to build Cyberspace/Signal/Electronic Warfare (EW) forces to conduct integrated cyberspace operations and EW; to develop Doctrine, Organization, Training, Material, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P) solutions, and to influence the Army's Science and Technology efforts that lead to capabilities that allow the Army to project power in and through cyberspace and the electromagnetic spectrum.

2. Previous Memorandums of Agreement. N/A

3. AUTHORITIES: 10 U.S.C. 2304(c)(3)(B)

4. PURPOSE: This MOU between the Cyber CoE and UCF is for the purpose of fostering a strategic relationship between said parties. The MOU also describes the objectives and scope of UCF-provided research capabilities, education, training and technical support for the Cyber CoE's mission to be Department of Defense's (DoD) recognized experts for cyberspace, signal, and EW, in order to develop DOTMLPF-P solutions that synchronize Warfighting Functions in converging land and cyberspace domains. It establishes the basic assumptions required to enable effective collaboration and support requirements. Each of the undersigned parties understands and agrees to support the objectives and uphold the responsibilities outlined in this MOU.

This MOU is intended to establish a mutually beneficial, cooperative relationship between USA Cyber CoE and Institution for the purposes of:

4.1. Developing a nationally recognized Cyber training and mission support capability.

4.2. Delivering education, training, and technical support in cyberspace operations, EW, spectrum management, network transport and information services, network operations, and other areas as determined by the Cyber CoE. Emphasis shall be placed on defensive and offensive cyberspace operations/cyber security, information dominance, information operations, Cyber-EW convergence, and the like. The intent for

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

curriculum development funding is not Tuition Assistance (TA). TA is regulated by DODI 1322.25, *Voluntary Educational Programs*.

4.3. Collaborating on and/or co-developing applicable cyberspace capabilities to support Training and Doctrine Command (TRADOC) Capabilities Managers and the Cyber Battle Lab (CBL), as the user representative and experimentation support, respectively, for U.S. Army Cyberspace Command (ARCYBER) Joint Force Headquarters-Cyber, and other Army cyberspace stakeholders (to include corps and below elements).

4.4. Jointly pursuing appropriate training, mission support, and participation in early acquisition insight test/experimentation venues.

4.5. Exploring internships and participation of students/trainees in relevant activities at each institution.

4.6. Developing courseware as needed and directed by the Cyber and Signal Schools for U.S. Army Career Management Fields (CMF) 25 Signal Corps (SC), 29 EW, 2210, and the new seventeen (17) (Cyber) career field and any other area of interest identified during collaboration.

4.7. Developing and executing formalized agreements and contractual documents between the parties, such as a Cooperative Research and Development Agreement, Cooperative Agreement, DoD IA Center Technical Area Task, or similar contractual vehicle to facilitate UCF support to Fort Gordon stakeholders.

5. RESPONSIBILITIES OF THE PARTIES: Specific course offerings and programs will be set forth in the terms of Program Level Agreements (PLAs) between the parties, which will define specific requirements, costs, billing arrangements, and other specifics as required. The Parties here-by agree that they will enter into negotiations for the establishment of PLAs for this purpose. The following responsibilities will be subject to the specific provisions of PLAs, and all regulations and policies applicable to each party's participation in each PLA.

5.1. The Cyber CoE will –

5.1.1. Assist Institution in curriculum development and participate as instructors during seminars and short courses when appropriate.

5.1.2. Provide facilities and equipment in support of these educational programs as needed and agreed upon.

5.1.3. Ensure students have the designated security classification for course requirements.

**Commented [HSL1]:** Will this eventually become a Memorandum of Agreement??

**Commented [k2R1]:** No, this will not become a MOA. This is the overarching agreement to start collaboration and anything project on curriculum design, research, etc may likely need an addition PLA/MOA to outline the roles, responsibilities and any funding requirements.

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

5.1.4. Facilitate student internships for degree, non-degree and professional education trainees. UCF students in certificate, Bachelor's and Masters degree programs frequently have a need for internship opportunities with industry, business, and government.

5.1.5. Collaborate with Institution in order to determine possible solutions for cyberspace operations, EW, and communication networks and information service and other area capability gaps.

5.2. UCF will –

5.2.1. Collaborate on the possible development of professional education short courses and facilitate undergraduate/graduate educational opportunities with the degree-granting organizations within the Institution to meet Cyber CoE needs.

5.2.2. Educational offerings may include but will not be limited to:

5.2.2.1. Short Courses. Continuing Education Units from Institution. Short courses do not require admission to the Institution but funding may be required.

Short/continuing education courses are educational programs that offer various options for on-line delivery and feature instructors such as university professors, civilian experts, and current cyber leaders from throughout the DoD. Courses are highly useful from an application point-of-view and will train participants in processes and tools needed to plan, monitor, and improve Cyber Security in their organization. The courses may be conducted either online, at the Institution's main campus in Orlando, Florida, at Fort Gordon, or at other mutually agreed upon locations.

For institutional training, specific course content can be tailored to the needs of the Cyber CoE. For example, current Institution credit-bearing course content can be leveraged for formal and informal training and would be complementary to the current Joint Cyber Analysis Course courseware with the added dimension of Institution faculty, who support cutting-edge DoD-funded cyber projects, conducting the bulk of the instruction or augmenting the instruction of DoD cyber security professionals. Upon completion of each continuing education course, students will receive an Institution certificate for the course taken.

5.2.2.2. Degree Programs. Each of the following degree programs requires admission to the Institution:

Bachelor's in Computer Science – designed for students seeking a four-year Bachelor's of Science degree, this curriculum includes the university's core curriculum, as well as advanced courses in information technology and cyber security.

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

Bachelor's in IT – designed for students seeking a four-year Bachelor's of Science degree, this curriculum includes the university's core curriculum, as well as advanced courses in IT and cyber security.

Master's in Digital Forensics – designed for students seeking a Master's of Science degree to be able to conduct analysis of computers and other types of digital media to determine if those devices have been used for illegal or unauthorized actions or if those devices have been attacked.

Graduate Certificate in Modeling and Simulation of Behavioral Cybersecurity – this five-course post-baccalaureate certificate builds on students' baccalaureate degrees and may also serve as a stepping-stone toward the Master of Science in Modeling and Simulation (Behavioral Cybersecurity track) or Doctor of Philosophy (Ph.D.) in Modeling and Simulation (Behavioral Cybersecurity track). Can be conducted face-to-face or fully online.

Master's in Modeling and Simulation (Behavioral Cybersecurity track) – designed for students seeking a Master's degree to evaluate the behavior of the human, organization, equipment, and/or systems under study through the evaluation of output from the corresponding simulation construct in behavioral cybersecurity operations.

Ph.D. in Modeling and Simulation (Behavioral Cybersecurity track) – designed for students seeking a Ph.D. to evaluate the behavior of the human, organization, equipment, and/or systems under study through the evaluation of output from the corresponding simulation construct in behavioral cybersecurity operations.

5.2.3. Facilitate internships for Cyber CoE professional educators.

5.2.4. During student institutional training graduation ceremonies, UCF shall have the opportunity to be on hand to present an official institutional certificate of training and possible transcripts.

5.3. To meet the objectives described above, both Parties agree to:

5.3.1. Assign Curriculum Development Coordinators (each party) for implementation of the Educational Development part of this MOU.

5.3.2. Explore ways to create an accredited articulated cooperative (program) covering Cyber degrees and certificates of training.

5.3.3. Investigate ways for non-degree seeking students to enroll in credit courses.

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

5.3.4. Develop courseware, as needed and directed by the Cyber and Signal Schools, for CMFs 25 (SC), 29 (EW), 2210,17 (Cyber) career fields (which may include non-classified and classified material) and any other area of interest identified during collaboration.

5.3.5. Explore the possibility of sponsoring an annual cyber security training event or other educational training events as identified in follow-on meetings (e.g., workshop, exercise, conference, etc.).

5.3.6. Establish quarterly meetings (alternating between locations or by audio or video teleconference/online participation if agreeable to both parties). The intent is to provide representatives from all organizations the opportunity for ongoing information sharing regarding current, planned, and/or new initiatives and activities.

5.3.7. Meet annually to review activities of the past year, and plans for the following year.

5.3.8. Adhere to each party's respective security rules and regulations when courses, meetings and conferences are hosted at Cyber CoE and the Institution.

5.3.9. Discuss ways to possibly sponsor an upcoming Army War College Fellowship at UCF/IST. If approved, it is slated to start in Fall Term, AY18-19.

6. PERSONNEL: Each Party is responsible for all of its personnel costs including pay and benefits, support, and travel. Each Party is responsible for supervision and management of its personnel. There will be no shared responsibility for management and/or supervision of personnel.

#### 7. GENERAL PROVISIONS:

7.1. POINTS OF CONTACT (POC): The Parties will use the following POC's in the implementation of this MOU. Each Party may change its POC upon reasonable notice to the other Party, and may appoint alternate POCs as needed.

7.1.1. For the Cyber CoE–

7.1.1.1. Primary: Ms. Gloria M. Palmer, G-8 – Support Agreement Manager, (706) 791-8753, gloria.m.palmer2.civ@mail.mil.

7.1.1.2. Alternate: Ms. Kimberly Burr, G-3/5/7, (706) 791-5482, kimberly.m.burr.civ@mail.mil.

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

7.1.2. For the Institution–

7.1.2.1. Primary: Dr. Bruce Caulkins, Program Director for the UCF M&S of Behavioral Cybersecurity Program, (407) 882-2427, bcaulkin@ist.ucf.edu.

7.1.2.2. Alternate: Ms. Mindy Solivan, Team Manager, Office of Research and Commercialization, University of Central Florida, (407) 882-0262, Mindy.Solivan@ucf.edu.

7.2. CORRESPONDENCE: The Parties will address all written correspondence sent or received specific to the content of this MOU as follows, unless directed otherwise:

7.2.1. For the Cyber CoE -

Department of the Army  
U.S. Army Cyber Center of Excellence (Cyber CoE)  
ATTN: ATZH-RM  
506 Chamberlain Ave  
Bldg 29808, Room 507  
Fort Gordon, GA 30905

7.2.2. For UCF -

Mindy Solivan  
University of Central Florida  
Office of Research and Commercialization  
12201 Research Parkway, Suite 501  
Orlando, FL 32826

7.3. MODIFICATION: This MOU may only be modified by the written agreement of the Parties, duly signed by their authorized representatives. Such amendments will be dated, consecutively numbered, and appended to each copy of this document.

7.4. EXPIRATION: This MOU expires five (5) years and one day after the signature of the last Party. If the agreement is to remain in effect after the five-year period, it can be re-signed in conjunction prior to the end of the five (5) year period.

7.5. TERMINATION: Either party may unilaterally terminate the agreement prior to the expiration date on sixty (60) days notice. If there are no PLAs in place and there are no outstanding issues involving reimbursement, this MOU may be unilaterally terminated by either party prior to the expiration date by providing thirty (30) days of advance notification. The MOU may also be terminated at any time upon the mutual written consent of the Parties.

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

7.6. NO TRANSFER: This MOU is not transferable except with the written consent of the Parties.

7.7. ENTIRE UNDERSTANDING: It is expressly understood and agreed that with the exception of any PLAs developed in accordance with this MOU, this MOU embodies the entire agreement between the Parties regarding the MOU's subject matter.

7.8. EFFECTIVE DATE: This MOU takes effect beginning on the day after the signature of the last Party.

#### 8. FINANCIAL DETAILS:

8.1. AVAILABILITY OF FUNDS: This MOU does not document the obligation of funds between the Parties. Any obligation of funds in support of this MOU will be accomplished as mutually agreed to by both Parties. The obligation of the funds by the Parties is subject to the availability of appropriated funds pursuant to the DoD Financial Management Regulation and the availability of funds appropriated and allocated to UCF, as determined in UCF's sole discretion.

8.2. BILLING: The institution will bill the lead organizations, as designated by the Cyber CoE, in accordance with the procedures established for products and/or services in the applicable PLA or as otherwise agreed upon by supplemental negotiation between the Parties. The Parties will maintain a record of the transactions by written/electronic correspondence between the Parties or by annual report after the month in which the first transaction occurred. Billing will be established in the applicable PLA or as otherwise agreed to by the Parties. Reimbursement will occur as mutually negotiated within the structure of the individual PLAs.

8.3. FINANCIAL SPECIFICS: See the applicable PLAs established in regard to agreed upon products and services or other supplemental agreements for details and information on the reimbursable support identified pursuant to the responsibilities identified in this MOU.

SUBJECT: Research, Training and Education between U.S. Army Cyber Center of Excellence (USA Cyber CoE) and UCF

In witness whereof, each of the parties have caused its authorized representative to execute this MOU on its behalf.

**THE UNIVERSITY OF CENTRAL FLORIDA BOARD OF TRUSTEES**

APPROVED:

FOR UCF -



MINDY SOLIVAN  
Team Manager  
UCF

08/31/2016

(Date)

FOR USA CYBER COE -

 Expired certificate

X Samuel G Anderson

Sam Anderson

Signed by: ANDERSON.SAMUEL.GRADY.III.1041756965

SAMUEL G. ANDERSON  
Colonel  
Chief of Staff

(Date)