

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE UNITED STATES ARMY CYBER CENTER OF EXCELLENCE (CYBER COE)
AND
GEORGIA TECH APPLIED RESEARCH CORPORATION (GTARC)
FOR
COLLABORATION IN PROVIDING CYBER RESEARCH, DEVELOPMENT, TRAINING, AND
EDUCATION

Cyber CoE #15-001

This is a Memorandum of Understanding (MOU) between the United States Army Cyber Center of Excellence (Cyber CoE) and Georgia Tech Applied Research Corporation (GTARC). When referred to collectively, they are referred to as the "Parties."

1. BACKGROUND:

1.1. As an Army-sponsored University Affiliated Research Corporation (UARC), Georgia Tech Research Institute (GTRI) is uniquely qualified and geographically positioned to support the mission needs of the U.S. Army Cyber CoE, located at Fort Gordon, GA. Per the Department of Defense (DoD) UARC Management Plan dated (July 2010), UARCs provide or maintain DoD essential engineering, research, and/or development core capabilities and maintain a long-term strategic relationship with DoD. The characteristics of this relationship are:

- Responsive and comprehensive knowledge of the sponsors requirements, and problems.
- Collaborative environment to share ideas, concepts, and emerging technologies.
- Broad access to information, including proprietary data.
- Broad corporate knowledge.
- Independence and objectivity.
- Quick response capability.
- Current operational experience.
- Freedom from real and/or perceived conflicts of interest.

1.2. Further, UARCs have Assistant Secretary of Defense for Research and Engineering (ASD (R&E) designated/approved core competencies, which are areas of expertise in key technical areas that support the UARC mission. The following GTRI UARC core competencies directly align with the mission needs of the U.S. Army Cyber CoE:

- Core Competency #8: System accessibility, susceptibility, and vulnerability analysis, modeling, and counter-countermeasure development.
- Core Competency #14: Basic and applied research, exploratory, and advanced

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

development in generic databases, networks, software engineering, telecommunications, and information infrastructure.

- Core Competency #16: Applied research in technologies affecting sustainment decision processes, secure communications, and communication systems.
- Core Competency #17: Analysis, systems engineering, integration, and rapid cyberspace tool development to address defensive/offensive cyberspace operations and cyber mission assurance requirements.

1.3. In addition to GTRI's UARC designation, GTRI is a non-profit organization of over 1,900 employees and serves as the applied research institute of Georgia Institute of Technology (GIT). As such, GTRI is an integral part of the University and has close partnerships with GIT colleges and faculty. In fact, all GTRI researchers are considered GIT faculty researchers and many are GIT adjunct teaching faculty. This unique relationship and construct allows GTRI to seamlessly partner with the degree-granting organizations within GIT and Georgia Tech Professional Education (GTPE), to facilitate degree and professional development education and training opportunities for the U.S. Army Cyber CoE.

1.4. REFERENCES.

1.1.1. Department of Defense Instruction (DODI) 4000.19, Support Agreements, 25 April 2013

1.1.2. Department of Defense University Affiliated Research Center (UARC) Management Plan, 23 June 2010

1.1.3. Department of Defense Strategy for Operating in Cyberspace, July 2011

1.1.4. Department of Defense Cyberspace Workforce Strategy, 04 December 2013

1.1.5. The Department of Defense Cyber Strategy, April 2015

1.5. PREVIOUS MEMORANDUMS OF AGREEMENT.

N/A.

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

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

3. PURPOSE: The U.S. Army Cyber CoE is pursuing a long-term, strategic partnership with GTARC to access 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.

This MOU between GTARC (a 501(c)(3) not-for-profit organization that serves as the contracting entity for GTRI) and the U.S. Cyber COE is for the purpose of fostering a strategic relationship between said parties. The MOU also describes the objectives and scope of GTARC-provided education, training and technical support for the Cyber CoE's mission to be *DoD's 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 understand and agree to support the objectives and uphold the responsibilities outlined in this MOU.

Hereinafter, the term "Institution" will refer to the collective GIT team comprised of GTRI and applicable entities within the degree and non-degree granting organizations within GIT and GTPE.

The objective of this MOU is to establish a mutually beneficial, cooperative relationship between GTARC and U.S. Cyber CoE for the purpose of:

- 3.1. Developing a nationally recognized Cyber training and mission support capability.
- 3.2. Delivering education, training, and technical support in cyberspace operations, electronic warfare, 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.
- 3.3. Collaborating on and/or co-developing applicable cyberspace capabilities to support Training and Doctrine Command (TRADOC) Capabilities Manager-Cyber (TCM-Cyber) and the Cyber/Network Battle Lab, as the user representative and experimentation support, respectively, for U.S. Army Cyberspace Command (ARCYBER) Joint Force Headquarters-Cyber (JFHQ-C), and other Army cyberspace stakeholders (to include corps and below elements).
- 3.4. Jointly pursuing appropriate training, mission support, and participation in early acquisition insight test/experimentation venues.
- 3.5. Exploring internships and participation of students/trainees in relevant activities at each institution.

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

3.6. 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 Electronic Warfare (EW), 2210, and the new 17 (Cyber) career fields.

3.7. Developing and executing formalized agreements and contractual documents between the parties, such as an Education Partnership Agreement, Cooperative Research and Development Agreement (CRADA), cooperative agreement, UARC contract, DoD Information Analysis Center (IAC) Technical Area Task (TAT), or similar contractual vehicle to facilitate GTARC support to Fort Gordon stakeholders.

4. RESPONSIBILITIES OF THE PARTIES:

4.1. The Cyber CoE will -

4.1.1. Assist in GTRI, GIT and GTPE curriculum development and participate as instructors during seminars and short courses when appropriate.

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

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

4.1.4. Facilitate internships for degree, non-degree and professional education trainees. GIT students in BS program and MS programs frequently have co-op and internship opportunities with industry/business/government.

4.1.5. Collaborate with GTRI in order to determine possible solutions for cyberspace operations, EW, and communication networks and information service capability gaps.

4.2. The Institution will -

4.2.1. Develop professional education short courses and facilitate undergraduate/graduate educational opportunities with the degree-granting organizations within GIT and GTPE to meet the needs of the U.S. Army Cyber CoE.

4.2.2. Educational offerings include but are not limited to:

4.2.1.1. **Short Courses:** Cyber Security Certificates & Continuing Education Units (CEUs) from GTPE

Short courses are educational programs that offer various options for on-line delivery; and feature speakers 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

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

their organization. The courses may be conducted at GTRI, GTPE, Fort Gordon, Savannah or other mutually agreed upon locations.

Specific course content shall be tailored to the needs of the U.S. Army Cyber CoE. For example, current content can be leveraged for formal and informal training and would be complimentary to the current Joint Cyber Analysis Course (JCAC) courseware with the added dimension of GTRI applied researchers, who support cutting-edge DoD-funded cyber projects, conducting the bulk of instruction with GIT resident instruction professors augmenting as needed. Upon completion of four courses, students will receive a GIT certificate from GTPE and CEUs for each course taken.

Examples of courses currently offered are as follows:

- Cyber Security: A Systems Approach
- Malware Analysis
- Mobile Device Security
- Network Security
- Cyber/EW Convergence
- Embedded Systems Design
- Exploitation and Defense of IT Systems: Hands on Lab
- Cyber Security of Embedded Systems
- Cyber Test and Evaluation
- Penetration Testing
- Incident Response
- Secure Software Development and Design
- Identification and Access Management
- Net-centric Command and Control

4.2.1.2. Degree Programs:

Masters of Science in Computer Science (MSCS): A full-tuition program offered on campus, only. Takes 18-24 months to complete and requires GIT admission. Has an Information Security specialization, but is not as detailed in the subject matter as MS InfoSec. Requires a BS in Computer Science, Electrical Computer Engineering, Math, or possibly Physics.

On-line MSCS (OMSCS): The main difference from the MSCS is that it is a low-tuition (~\$7,000) online program.

Masters of Science in Information Security (MS InfoSec): Offered on-campus and via Distance Learning (synchronously transmitted lectures taped in the classroom; asynchronously available online). Both programs require a Bachelors of Science (BS) in Computer

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

Science, Electrical Computer Engineering, Math, or possibly Physics.

BS in Computer Science: On-campus, full-tuition program. Takes 4 years to complete and requires GIT admission.

4.2.1.3. Non-Degree, Special Status students: It is possible for students to be admitted as non-degree students and register for classes on-campus, online, or via distance learning. These students would participate with other students in classes and get a GIT transcript with letter grades and credit hours recorded. They could also receive a certificate from GTPE for taking 4 classes.

4.2.3. Facilitate internships for the professional educator.

4.2.4. Conduct boot camp courses for personnel needing preparatory classes before joining degree programs.

4.2.5. Brief and initiate the evaluation/enrollment process for new students prior and during all new Cyber training start-up sessions.

4.2.6. During Cyber student Graduation ceremonies, the Institution shall be on hand to present an official institutional certificate of training and possible transcripts containing the regional awarded college credit for the dual enrolled courses and/or residential on-line institutional required courses.

4.2.7. During the Annual Post Graduation Ceremony (normally in June of each year), the Institution shall present diplomas or confer degrees to those candidates who meet the requirement.

4.2.8. Research Security will provide on-site security support when Army Cyber CoE attends courses, meetings and conferences at the Institution. This support will include but not limited to: Visitor Control, Document Control, Information Assurance, Physical Security and Operations Security.

4.2.9. Present and provide an understanding of cyberspace, EW, and communications networks and information service efforts that GTRI is prototyping that may address Army related requirements and gaps.

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

4.3.1. Identify an Institution senior faculty member and Cyber CoE senior leader as the principal point of contact (or liaison) in each party to apprise the MOU signatories with the progress of collaboration.

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

- 4.3.2. Assign Curriculum Development Coordinators (each party) for implementation of the Educational Development part of this MOU.
- 4.3.3. Create an accredited articulated cooperative (program) both covering Cyber degrees and certificates of training.
- 4.3.4. Continue sharing non-proprietary information through a GTRI/Cyber CoE SharePoint or similar file transfer portal.
- 4.3.5. Investigate ways for non-degree seeking students to enroll in credit courses.
- 4.3.6. Develop courseware as needed and directed by the Cyber and Signal Schools for CMFs 25 (SC), 29 (EW), 2210, and 17 (Cyber) career fields (which may include non-classified and classified material).
- 4.3.7. Explore the sponsoring of an annual cyber security training event (e.g., workshop, exercise, conference, etc) at the GTPE Global Learning Center, GTRI Conference Center, GTRI's secure collaborative facilities, the Georgia Tech Savannah campus or at Fort Gordon.
- 4.3.8. Establish quarterly meetings (alternating between locations or by conference/teleconference/VTC/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.
- 4.3.9. Meet annually to review activities of the past year, and plans for the following year.
- 4.3.10. An on-line co-enrollment with the Institution when Service members are assigned to Fort Gordon for formal Cyber and/or Signals training.
- 4.3.11. Develop and execute between the parties a contractual vehicle(s) to facilitate timely GTARC support to Fort Gordon stakeholders.
- 4.3.12. Adhere to each party's respective security rules and regulations when courses, meetings and conferences are hosted at Cyber CoE and the Institution.

5. 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.

6. GENERAL PROVISIONS:

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

6.1. POINTS OF CONTACT: The Parties will use the following Points of Contact (POC) in the implementation of this MOU. Each Party may change its POC upon reasonable notice to the other Party.

6.1.1. For the Cyber CoE—

Primary POC: Ms. Gloria Palmer, G-8, (706) 791-8753,
gloria.m.palmer2.civ@mail.mil.

Alternate POC: Ms. Kimberly Burr, DOT, (706) 791-5482,
kimberly.m.burr.civ@mail.mil.

6.1.2. For the Institution—

<u>NAME</u>	<u>TITLE</u>	<u>EMAIL</u>	<u>PHONE</u>
Stephen Moulton	Institution Liaison to Ft Gordon	stephen.moulton@gtri.gatech.edu	757-634-6828
Dr. Mustaque Ahamed	Curriculum Development Coordinator	mustaque.ahamad@cc.gatech.edu	404-894-2593
Dr. Leo Mark	Assoc Dean, Acad/Student Affairs	leo.mark@pe.gatech.edu	404-407-6067
Dr. James Wilburn	Military Academic Pgm Dir	james.wilburn@pe.gatech.edu	912-966-7951
Ms. Jennifer Wooley	Dir, Prof Master's Programs	jennifer.wooley@pe.gatech.edu	404-385-7460
Dr. Fred Wright	GTRI Cyber Prof Education	fred.wright@gtri.gatech.edu	404-407-7296
Ms. Renita Folds	GTRI Cyber Prof Education	renita.folds@gtri.gatech.edu	404-407-7253
Mr. Albert Concord	FSO/Security Director	al.concord@gtri.gatech.edu	404-407-7998
Ms. Lucy Yarborough	Contracting Officer	lucy.yarbrough@osp.gatech.edu	404-385-2084

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

6.2.1. For the Cyber CoE -

Department of the Army
U.S. Army Cyber Center of Excellence (Cyber CoE)
ATTN: ATZH-DT
506 Chamberlain Ave
Bldg 29808, Room 813
Fort Gordon, GA 30905

6.2.2. For the GTARC -

Georgia Tech Applied Research Corporation (GTARC)
ATTN: Lucy Yarborough
505 Tenth Street
Atlanta, GA 30332-0420

6.3. MODIFICATION OF UNDERSTANDING: 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.

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

6.4. **DISPUTES:** Any disputes relating to this MOU will, subject to any applicable law, Executive Order, Directive, or Instruction, be resolved by consultation between the Parties or in accordance with DoDI 4000.19.

6.5. **TERMINATION OF UNDERSTANDING:** Either party may unilaterally terminate the agreement prior to the expiration date only with sufficient advance notification, a minimum of 180 days, to permit appropriate resource adjustments to be made during the budget formulation process. If an agreement involves reimbursement or if resources must be significantly modified or unilaterally terminated with less than 180 days' notice to the other party or parties to the agreement, the party requiring the modification or termination may be billed by the supplier in accordance with the terms of the applicable agreement for reimbursement. If there are no agreements 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 30 days of advance notification. The MOU may also be terminated at any time upon the mutual written consent of the Parties.

6.6. **TRANSFERABILITY:** This MOU is not transferable except with the written consent of the Parties.

6.7. **ENTIRE UNDERSTANDING:** It is expressly understood and agreed this MOU embodies the entire agreement between the Parties regarding the MOU's subject matter.

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

6.9. **EXPIRATION DATE:** This MOU expires nine years and one day after the signature of the last Party. If the agreement is to remain in effect after the nine-year period, it can be re-signed in conjunction with the third triennial review.

6.10. **CANCELLATION OF PREVIOUS AGREEMENT:** N/A.

7. **FINANCIAL DETAILS:**

7.1. **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.

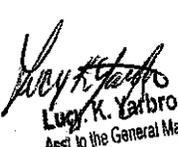
7.2. **BILLING:** The institution will bill the lead organizations, as designated by the Cyber COE, in accordance with the procedures established for products and/or services in the applicable Program Level Agreements (PLA) or as otherwise agreed upon by supplemental negotiation between the Parties. 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.

SUBJECT: Cyber CoE and GTARC Collaboration in Conducting Cyber Research, Development, Training, and Education, Cyber MOU # 15-001

7.3. PAYMENT OF BILLS: Reimbursement will occur as mutually negotiated within the structure of the individual PLAs.

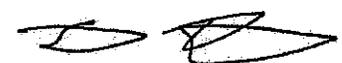
7.4. FINANCIAL SPECIFICS: See the applicable PLA(s) established in regard to agreed upon products and services or other supplemental agreements for details and information on the reimbursable support identified pursuant to the responsibilities identified in paragraph 4 of this MOU.

AGREED:

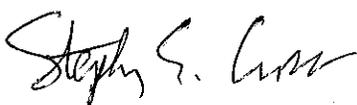

Lucy K. Yarbrough
Asst to the General Manager


LINDA GARTON
VP Research
Director
Office of Sponsored Programs
Georgia Institute of Technology

9/9/15
(Date)


STEPHEN G. FOGARTY
Major General, U.S. Army
U.S. Army CYBER Center of Excellence

28 AUG 2015
(Date)


STEPHEN E. CROSS, Ph.D.
Executive Vice President of Research
Georgia Institute of Technology

9/10/2015
(Date)


AL CONCORD
Director/Facility Security Officer
Research Security
Georgia Tech Research Institute

9 Sept 2015
(Date)