Center for Excellence in Cybersecurity

1.0 Name of the proposed center
Center for Excellence in Cybersecurity

2.0 Background
Research and education in cybersecurity focuses on protecting networks, programs and data from attack, damage or unauthorized access and recovery from an attack, should one happen. As threats that exploit vulnerabilities in our cyberinfrastructure grow and evolve, an integrated cybersecurity workforce must be capable of designing, developing, implementing, and maintaining both defensive and offensive cyber strategies.

Academic institutions are a critical part of preparing and educating the cybersecurity workforce. Collaboration among public and private entities enables academic institutions to determine requisite common knowledge and abilities. In response, institutions of higher education conduct research and develop and deliver curricula that prepares students with the skills needed by employers. As the complexity and demands of cybersecurity increase, more students will be attracted to academic cybersecurity programs as a pathway to a career. Therefore, qualified faculty and adequate laboratory resources are critical to not only teach the students, but to stay current by performing cutting-edge research in which the students can also participate.

Cybersecurity research and education may be studied on three different levels. First, cybersecurity is understood as a technical discipline evolving out of mathematics, statistics, computer science, and information technology. In that respect, it centers around intrusion detection and prevention; cloud security; system exploitation; cryptography; big data analytics; social network analysis; human language technology; visual analytics; data sensing and fusion; human-machine interaction; and high-performance secure computing. Second, cybersecurity can only be effective when technical approaches are married with effective social and economic policies; criminal justice and law enforcement; international trade and tourism; understanding of languages; international relations, flow of goods and data in a borderless society; study of customs, beliefs and faiths; and global agreements to find solutions in a cultural context. Finally, it is helpful to study cybersecurity in the context of an industry sector or a specific social or commercial application such as banking, travel, healthcare, polling and elections, cyber-physical systems and IoT manufacturing, and the electric grid. Data breaches in each such sector carry unique challenges and demand different approaches for protecting data and for mitigating the impacts after a breach.

This strategic plan for cybersecurity research, development and education over the next five years articulates a commitment from the University to advance its existing research culture and agenda to a higher level in line with the A&T Preeminence 2023 goals. The successful implementation of this strategic plan will require the engagement of a large cross section of the university including faculty, staff and students belonging to all academic colleges, and administrators and staff from most of the administrative divisions.

3.1 Need for Center
Cybersecurity research and education is a growing interest area at North Carolina A&T and will continue to grow in terms of external funding opportunities and student employment openings. In order to respond meaningfully to the opportunities, there is a need to have a strong unified approach that builds on the collective strengths of many faculty in several academic departments across the campus. To date most of the work in this area has been performed in a few academic departments without a single coordinated strategy at the university level. For example, biometrics is taught in the computer science department with research conducted in the Center for Advanced Identity Sciences

(CASIS) and Center for Cyber Defense (CCD). Four different academic departments in two colleges are currently responsible for courses and curricula: Data science is taught in the Mathematics department, visualization in Computational Science and Engineering department, artificial intelligence and machine learning in the Computer Science department and network security in the Computer Systems Technology department. Establishing a center will provide the structure and resources to enhance N. C. A&T's positioning and reputation in cybersecurity thereby leading to greater opportunities for faculty and students.

3.2 Scope

The Center will advance all aspects of scholarly cybersecurity research, education and outreach through collaboration across the university's academic units; partnerships with educational and research institutions and private industry; education and engagement of undergraduate and graduate students; workforce training, development of intellectual property and technology transfer; research dissemination; testing and evaluation; consultation; incident response and forensics; awareness and outreach to the general community and public media.

While the Center's scope will eventually broaden and grow over time, it will begin with research and education through five thrust areas, each with its own thrust leader: data visualization; biometrics; big data analytics; artificial intelligence and machine learning; and public policy to include expertise from social, political, economic, business and criminal justice.

Visualization: Data visualization uses algorithms to create images from data so humans can understand and respond to that data more effectively. Artificial intelligence and machine learning is the quest for algorithms that can understand and respond to data the same way as a human can or better. The Center will investigate how machine learning can improve data visualization as well as how it can improve the security of large amounts of visualization data.

Biometrics: Biometrics can be classified as the automated recognition of individuals based on their behavioral or biological characteristics. The main advantage of physiological biometrics is permanence, that is, most of the features it draws on are stable and do not vary with time. Fingerprints, for example, don't change, nor do the unique scannable patterns of our eyes. A large majority of data breaches result from weak authentication protocols that allow cybercriminals to obtain the credentials of users and gain access to an organization's most valuable assets within their IT infrastructure. The Center will continue research in biometrics and expand by applying machine learning techniques.

Big Data Analytics: Information and business data are among the most valuable assets of any company and therefore their protection is of paramount importance. Big data analytics professionals are making use of preventative technologies as well as managed detection and response services. Companies use these to deal with the constantly evolving, sophisticated cyberthreats caused by the increased amounts of data being generated on a daily basis. The use of big data analytics enables deep analysis of the information collected. Ultimately, this gives hints of a potential threat to the integrity of the company. With such analysis, businesses can know when there is a deviation from the norm using the data collected. New statistical and predictive models and possibilities can also be created using this historical data by the use of artificial intelligence and machine learning.

Artificial Intelligence and Machine Learning: Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention. Machine learning networks are making significant improvements to the existing information security solutions. Malware detection and network intrusion detection are two such areas where deep learning has shown significant improvements over the rule-based solutions. The Center will investigate various

techniques aimed at protecting large data sets.

Public policy: Increasingly, cybersecurity is being treated as a national and public safety priority. While technical approaches have focused on countering the threat of cyber-attacks, policy decisions have ranged from the short term focus on costs to discussions regarding restricting access to malevolent actors and the precise mechanisms that would permit such restrictions. Since computers and their networked operations are the lifeblood of business and government, the sectors of transportation, health care, banking, energy, national defense, space exploration, etc. are all vulnerable to criminals and terrorists. Experts in social, political, economic, business and criminal justice disciplines can address a wide range of important questions, for example, the loss of intellectual property through cyber espionage, the cost of not reporting cyber intrusion, civil liberties concerns when government authorities conduct surveillance of data networks, and the invasion of privacy not only when personal data is stolen but also when large data sets from two or more databases are combined to identify personal details about individuals.

The thrust areas will be advanced through interdisciplinary teams of faculty, staff and students that will result in the development of cybersecurity resources for the larger university community, provide research and innovation in cybersecurity, and offer education and outreach in cybersecurity.

Resource Development: The Center will take advantage of high performance computing and visualization resources currently located in Fort IRC, Cherry Hall, and JSNN and supplement them with additional tools for education and research in cybersecurity including servers, switches and networking hardware, cyber ranges, software development platforms, and testing tools.

Research and Innovation: The Center will unify the university's current research capability in biometrics, visual recognition, artificial intelligence and machine learning to create an environment for faculty and students to explore cross-cutting applications in information security. The Center will collaborate with academic department to engage graduate students and post-doctoral scholars in advanced research, sponsor seminars and workshops.

Education and outreach: The Center will provide expertise, training, and support for faculty, students and professionals to enhance their skills in cybersecurity technology and policy. The Center will offer workshops on data visualization, biometrics, big data analytics, artificial intelligence and machine learning as applied to the security of large datasets. In addition, the Center will establish a forum for intellectual discussions and research on the social, economic, and cultural factors associated with cybersecurity. The Center will increase public awareness of cybersecurity concerns and will maintain a dashboard to indicate current vulnerabilities and threats while offering prevention strategies and remedies to those who have been attacked.

3.3 Mission

The Center will be the academic and research nexus for the development of advanced mathematical and computational techniques and investigation of socioeconomic practices related to cybersecurity and security of large data sets. The purpose of the Center is to advance the state of the art to anticipate future cyber-attacks, to secure valuable datasets, and to offer strategies for recovering from a cyber attack. The center will provide a unique framework for partnerships between academia, government and industry on research programs of various sizes and applications. Advances in education and research in this field will provide students and faculty with opportunities to participate in interdisciplinary programs, and to prepare for careers in the burgeoning field of cybersecurity to serve industry and government needs across the Piedmont Triad region, the state of North Carolina and the United States.

3.4 Objectives

The objectives of the Center are to

a. Conduct research leading to development of advanced cybersecurity technologies
b. Develop technologies and best practices for securing visual and biometric data from cyberattacks
c. Provide education and training in visual and biometric data security
d. Advise deans and provost on faculty competencies in faculty hiring and professional development leading to the creation of an interdisciplinary community of cybersecurity experts
e. Serve as a workforce development pipeline for students with a background in cybersecurity
f. Support the creation of new cybersecurity business and high skill jobs in the region and state

4.0 Relationship to University Mission

The Center is fully aligned with the university's strategic plan (Preeminence 2023).

4.1 Preeminence 2023 Goal 1: Excellence in Teaching, Research and Student Success

The creation, storage, and visualization of large data sets generated in military, commercial, manufacturing, healthcare, and financial applications have led to increased concerns for data security. In responding to these concerns, the Center will enhance the faculty's ability to conduct cutting edge research and to offer advanced courses that combine data visualization, artificial intelligence, machine learning, along with an emphasis on social, cultural, political and economic factors to advance the nation's ability to counter the threat of cybercrime and cyberterrorism. The Center will provide advanced approaches to predicting and mitigating cyber attacks intending to distort or destroy visual and biometric data. The convergence of computational methods to autonomously protect the integrity of data driven systems is emerging as a key field of study. Advances in education and research in this field will provide students and faculty with opportunities to create interdisciplinary programs, prepare for careers in a burgeoning field, and innovate in interdisciplinary applications where visual and biometric information is critical.

4.2 Preeminence 2023 GOAL 2: Intellectual Climate

The Center will provide a focal point for cybersecurity related research, education and training on the campus. As part of its operations, the Center will conduct workshops, seminars, conferences, and invited lectures to educate both the scientific and technical community and the population at large. In doing so, the Center will attract more faculty and students to the important field of cybersecurity, help the university recruit more students and research scientists, and create an environment for faculty and students to explore cross-cutting applications. All these activities will enhance the intellectual climate on campus.

4.3 Preeminence 2023 GOAL 3: Public Service and Community Engagement

The Center will serve as a point of expertise on cybersecurity and security of large data sets in general and biometric cybersecurity in particular. The Center will also support the growing cybersecurity industry in the state and Piedmont Triad region as well as federal efforts across a variety of agencies that are or will be using visual and biometric information in analysis and decision- making.

4.4 Preeminence 2023 GOAL 4: Stewardship, Operational Effectiveness and Efficiencies

The Center will initially use the resources of the existing High-Performance Computing (HPC) facilities that already exist on campus including any associated visualization systems. In order to most efficiently use these resources, it is anticipated that HPC systems could be used by the Center in off-peak periods. In the future, it may be necessary to acquire dedicated HPC resources due to load requirements or to isolate computer systems due to government or corporate security requirements.

5.0 Differentiation from similar centers within N.C. A&T and/or UNC system

The Center will be closely related to the CASIS and CCD centers and will provide a long term institutional structure to CASIS and CCD since they are formed as a result of specific contracts and grants and their life is highly dependent on renewal of single sponsored awards. The Center will also benefit from the resources available in the Visualization and Computation Advancing Research (ViCAR) Center that provides expertise in computational environments, applications and software development, parallel and GPU programming, and scientific visualization. The ViCAR Center offers scalable, high performance massively parallel performing and cluster computers, mid range servers, a large screen 3D stereo vision visualization system with tracking, and software licenses for computational science users including Mathematica, COMSOL, AVS/Express, PDF3D, and VRCO.

A review of the universities in the UNC System indicates that all but two offer a bachelor's degree, ten offer an MS and four (N. C. A&T, NC State, UNC Charlotte and UNC Chapel Hill) offer a PhD in computer science or information systems. NC State University has centers on bioinformatics, geospatial analytics, scientific computation, advanced analytics, and next generation IT systems. UNC Charlotte has a center on bioinformatics, and one on visualization. UNCG has a center on data evaluation and analytics. UNC Wilmington has a center for identity sciences and is a collaborating center with A&T's CASIS Center. The proposed Center at NCA&T will develop partnerships with NC State, UNC Chapel Hill, UNC Charlotte and UNC Wilmington in effectively using equipment and expertise and in joint funding proposals

6.0 Relationship with academic programs

With its initial emphasis on biometrics, visual recognition, artificial intelligence, and machine learning to create cross-cutting applications in cybersecurity, the Center will naturally be more closely aligned with the following academic programs.

- Applied Mathematics
- Applied Science and Technology – Bioscience, Data Science and Analytics, Information Technology
- Computer Science
- Computational Science and Engineering
- Electrical Engineering
- Computer Engineering
- Industrial and Systems Engineering
- Information Technology
- Economics
- Criminal Justice

The Center will continue to enhance its relationship with these programs as it builds new partnerships with a larger cross section of academic programs. The Center will identify current courses in cybersecurity and will continue to assist academic departments by advising them of new developments and course enhancements and in further strengthening their portfolio of course offerings. A partial listing of cybersecurity related courses in provided below; this list will be continually updated by the Center and promoted on its website.

- ABM 406 - Quantitative Anal in Agribusiness
- ABM 436 - Agricultural Prices and Forecasting
- ABM 705 - Statistical Meth for Agriculture
- ABM 708 - Econometrics in Agribusiness
- ANSC 771 Bioinformatics Genome Analysis
- Applied Science and Technology – Data Science and Analytics
- COMP 320: Fundamentals of Cyber Security
- COMP 365 - AI and Machine Learning

- COMP 420. Applied Network Security
- COMP 468 - Introduction to Data Mining
- COMP 620: Information, Privacy and Security
- COMP 621: Web Security
- COMP 651 Data Analytics Techniques
- COMP 725: Software Security Testing
- COMP 726: Network Security
- COMP 727: Secure Software Engineering
- COMP 851 - Big Data Analytics
- COMP 878. Usable Security
- COMP765 Data Mining
- CSE 701- Appl Probability & Statistics
- CSE 801- Computational Statistics
- CSE 804- Computational Modeling and Visualization
- CSE 805- Machine Learn and Data Mining
- CST 225 -- Computer Database Management I
- CST 306 -- Big Data Analytics
- CST 325 -- Computer Database Management II
- CST 625 -- Computer Database Management
- CST 729 -- Data Warehousing
- CST 759 -- Big Data Analytics
- ECEN 651, 657 Signal and image processing
- ECEN 857 Pattern recognition
- ECEN 867, 868, 880 NeuralNnetworks
- MATH 224, 365, 608, 623, 624, 706, 708, 721, 723, 781 & 782
- PHYS 497, 746
- PSYC 150: Information Processing Techniques in Behavioral Research
- PSYC 250: Psychological Statistics
- PSYC 252: Applications of Psychological Statistics
- PSYC 447: Special and Contemporary Topics in Behavioral Data Analytics
- PSYC 450: Advanced Statistics and Computer Applications
- SOCI 203 Social Statistics I
- SOCI 213 Social Statistics II
- SOCI 310 Research Methods I
- STAT 324, 328, 423, 424, 425, 426

7. Structure and Organization

The Center will be led by a Center Director who will report to the Senior Vice Provost for Academic Affairs. The Center Director shall have a tenured faculty appointment in one of the academic departments but will receive half-time release time to conduct the work of the Center. The Center Director is responsible for all management and operations functions, and for the success of the Center. The Center Director will work closely with the Deans and Chairs of all colleges and departments to form a leadership team, as well as to identify all funded research and faculty with relevance to the Center's mission. The Center Director will recruit and hire additional research staff and post-doctoral fellows to carry out the Center's mission. The Center Director is responsible for developing and fostering strong relationships with university and industry partners. The Center Director will also meet regularly with the Faculty Advisory Committee, and meet once a year with the Steering Committee and the External Advisory Board for guidance and counsel.

The Center Director will be assisted by a Postdoctoral Research Associate and a graduate student administrative assistant.

The Steering Committee will consist of the Provost, Senior Vice Provost, Vice Chancellor for Research and Economic Development, and all the Deans of colleges that have affiliated faculty members. The committee will facilitate the work of the Director by helping with collaborations among academic units, development of courses and degree programs, and formation of interdisciplinary research teams. The Steering Committee also conducts periodic assessment of the effectiveness of the Center in meeting identified needs and program goals.

The External Advisory Board will consist of representatives of funding agencies, government and civic bodies, and industry representatives. The External Advisory Board advises the Center Director on strategic directions and priorities and assists in identifying resources required to address priority research, outreach and teaching needs. The Board assists in identifying resources and funding opportunities for Center activities.

Appendix 1: Faculty Listing

Faculty

The following list includes all faculty who either have active research programs, have been nominated by their respective Dean, or have expressed an interest in developing research programs in cybersecurity. Their academic background, current research strengths, and future funding opportunities should guide future faculty hiring plans.

Agriculture and Environmental Sciences

1. Dr. Kenrett Jefferson-Moore
2. Dr. Uchenna Y Anele
3. Dr. Kathleen (Chi Lyi) Liang
4. Dr. Mulumebet (Millie) Worku
5. Dr. Shengmin Sang
6. Dr. Reza Tahergorabi
7. Dr. Niroj Aryal
8. Dr. Guochen Yang
9. Dr. Salam Ibrahim
10. Dr. Yewande Fasina

Business and Economics

11. Dr. Alexander Yap
12. Dr. Stephanie Kelly
13. Dr. Lyubov Kurkalova
14. Dr. Mary Lind
15. Dr. Hayward Andres
16. Dr. Belinda Shipps
17. Dr. Hong Wang
18. Dr. George Stone
19. Dr. Jacqueline Williams

Engineering

20. Dr. Tonya Smith-Jackson
21. Dr. Raymond Tesiero
22. Dr. Dukka Kc
23. Dr. Marwan Bikdash
24. Dr. Hyoshin Park
25. Dr. Mohd Anwar
26. Dr. Albert Esterline
27. Dr. Kaushik Roy
28. Dr. Allison Sullivan
29. Dr. Xiaohong Yuan
30. Dr. Huiming Yu
31. Dr. Jinsheng Xu
32. Dr. Dr. Christopher Doss
33. Dr. Abdollah Homaifar
34. Dr. Ali Karimoddini
35. Dr. Abdullah Eroglu

36. Dr. Lauren Davis
37. Dr. Steven Jiang
38. Dr. Paul Stanfield
39. Dr. Hyung Nam Kim
40. Dr. Chrysafis Vogiatzis
41. Dr. Sun Yi

Science and Technology

42. Dr. Li-Shiang Tsay
43. Dr. Qing-An Zeng
44. Dr. Clay Gloster
45. Dr. Guoqing Tang
46. Dr. Liping Liu,
47. Dr. Kossi Edoh
48. Dr. Suzanne O'Regan
49. Dr. Sayed Mostafa
50. Dr. John Paul Ward
51. Dr. Seong-Tae Kim
52. Dr. Giles Warrack
53. Dr. Ling Xu
54. Dr. Gasparian
55. Dr. Abdellah Ahmidouch
56. Dr. Ron Perdoni

Arts, Humanities and Social Sciences

57. Dr. George Johnson
58. Dr. Arwin Smallwood

Health and Human Sciences

59. Dr. Joseph Stephens
60. Dr. George Robinson
61. Dr. Stephanie Teixeira-Poit

Bluford Library

62. Dr. David Rachlin

Nanoengineering

63. Dr. Ram Mohan
64. Dr. Kristin Rhinehardt