Senate Bill 1819-03

UNIVERSITY SENATE

UNIVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK

Introduced by: Graduate Academic Council
University Planning & Policy Council

Date: October 24, 2018

PROPOSAL TO ESTABLISH A MASTER OF SCIENCE (M.S.) PROGRAM IN DIGITAL FORENSICS AND CYBERSECURITY

IT IS HEREBY PROPOSED THAT THE FOLLOWING BE ADOPTED:

1. That the University Senate approves the attached proposal to establish a M.S. program in Digital Forensics and Cybersecurity as approved by the Graduate Academic Council (10/22/18) and University Planning & Policy Council (10/19/16).

2. That this proposal be forwarded to the President for approval.

MEMORANDUM

TO: James Mower, Senate Chair

FROM: Havidán Rodríguez, President

DATE: November 14, 2018

SUBJECT: Senate Bill Approval

I am pleased to approve the following Senate Bill, which was recommended following approval by the University Senate at its meeting of October 15, 2018:

Senate Bill 1819-03: PROPOSAL TO ESTABLISH A MASTER OF SCIENCE (M.S.) PROGRAM IN DIGITAL FORENSICS AND CYBERSECURITY

Approved: _____

Havidán Rodríguez, President

oo

SUNY The State University of New York

New Program Proposal: Graduate Degree
Program Form 2B
Version 2016-10-13

This form should be used to seek SUNY's approval and New York State Education Department's (SED) registration of a proposed new academic program leading to master's or doctoral degree. Approval and registration are both required before a proposed program can be promoted or advertised, or can enroll students. The campus Chief Executive or Chief Academic Officer should send a signed cover letter and this completed form (unless a different form applies[1]), which should include appended items that may be required for Sections 1 through 6, 9 and 10 and MPA-1 of this form, to the SUNY Provost at *program.review@suny.edu*. The completed form and appended items should be sent as a single, continuously paginated document.[2] If Sections 7 and 8 of this form apply, External Evaluation Reports and a single Institutional Response should also be sent, but in a separate electronic document. Guidance on academic program planning is available here.

Table of Contents

NOTE: Please update this Table of Contents automatically after the form has been completed. *To do this, put the cursor anywhere over the Table of Contents, right click, and, on the pop-up menus, select "Update Field" and then "Update Page Numbers Only." The last item in the Table of Contents is the List of Appended and/or Accompanying Items, but the actual appended items should continue the pagination.*

---

[1] Use a different form if the proposed new program will lead to a graduate degree or any credit-bearing certificate; be a combination of existing registered programs (i.e. for a multi-award or multi-institution program); be a breakout of a registered track or option in an existing registered program; or **lead to certification as a classroom teacher, school or district leader, or pupil personnel services professional** (e.g., school counselor).

[2] This email address limits attachments to 25 MB. If a file with the proposal and appended materials exceeds that limit, it should be emailed in parts.

Section 1. General Information		
a) Institutional Information	Date of Proposal:	September 2018
	Institution's 6-digit SED Code:	210500
	Institution's Name:	University at Albany, SUNY
	Address:	1400 Washington Ave., Albany, NY 12222
	Dept of Labor/Regent's Region:	Capital Region
b) Program Locations	List each campus where the entire program will be offered (with each institutional or branch campus 6-digit SED Code): Albany, 210500	
	List the name and address of off-campus locations (i.e., extension sites or extension centers) where courses will offered, **or check here [X] if not applicable**:	
c) Proposed Program Information	Program Title:	Digital Forensics and Cyber Operations
	Award(s) (e.g., M.A., Ph.D.):	M.S.
	Number of Required Credits:	Minimum [36] If tracks or options, largest minimum [ ]
	Proposed HEGIS Code:	0799
	Proposed 6-digit CIP 2010 Code:	11.1003
	If the program will be accredited, list the accrediting agency and expected date of accreditation:	
	If applicable, list the SED professional licensure title(s)[3] to which the program leads:	
d) Campus Contact	Name and title: Jonathan Bartow, Vice Dean for Graduate Education Telephone:518.437.5062 E-mail:jbartow@albany.edu	
e) Chief Executive or Chief Academic Officer Approval	**Signature affirms that the proposal has met all applicable campus administrative and shared governance procedures for consultation, and the institution's commitment to support the proposed program.** ***E-signatures are acceptable.*** Name and title: James R. Stellar, Senior Vice President for Academic Affairs and Provost Signature and date:	
	If the program will be registered jointly[4] with one or more other institutions, provide the following information for each institution:	
	Partner institution's name and 6-digit SED Code: Name, title, and signature of partner institution's CEO (or **append** a signed letter indicating approval of this proposal):	

[3] If the proposed program leads to a professional license, a specialized form for the specific profession may need to accompany this proposal.
[4] If the partner institution is non-degree-granting, see SED's CEO Memo 94-04.

Attestation and Assurances

On behalf of the institution, I hereby attest to the following:

That all educational activities offered as part of this proposed curriculum are aligned with the institutions' goals and objectives and meet all statutory and regulatory requirements, including but not limited to Parts 50, 52, 53 and 54 of the Rules of the Board of Regents and the following specific requirements:

That credit for study in the proposed program will be granted consistent with the requirements in §50.1(o).

That, consistent with §52.1(b)(3), a reviewing system has been devised to estimate the success of students and faculty in achieving the goals and objectives of the program, including the use of data to inform program improvements.[5]

That, consistent with §52.2(a), the institution possesses the financial resources necessary to accomplish its mission and the purposes of each registered program, provides classrooms and other necessary facilities and equipment as described in §52.2(a)(2) and (3), sufficient for the programs dependent on their use, and provides libraries and library resources and maintains collections sufficient to support the institution and each registered curriculum as provided in §52.2(a)(4), including for the program proposed in this application.

That, consistent with 52.2(b), the information provided in this application demonstrates that the institution is in compliance with the requirements of §52.2(b), relating to faculty.

That all curriculum and courses are offered and all credits are awarded, consistent with the requirements of §52.2(c).

That admissions decisions are made consistent with the requirements of §52.2(d)(1) and (2) of the Regulations of the Commissioner of Education.

That, consistent with §52.2(e) of the Regulations of the Commissioner of Education: overall educational policy and its implementation are the responsibility of the institution's faculty and academic officers, that the institution establishes, publishes and enforces explicit policies as required by §52.2(e)(3), that academic policies applicable to each course as required by §52.2(e)(4), including learning objectives and methods of assessing student achievement, are made explicit by the instructor at the beginning of each term; that the institution provides academic advice to students as required by §52.2(e)(5), that the institution maintains and provides student records as required by §52.2(e)(6).

That, consistent with §52.2(f)(2) of the Regulations of the Commissioner of Education, the institution provides adequate academic support services and that all educational activities offered as part of a registered curriculum meet the requirements established by state, the Rules of the Board of Regents and Part 52 of the Commissioner's regulations.

CHIEF ADMINISTRATIVE or ACADEMIC OFFICER/ PROVOST

Signature	Date
Type or print the name and title of signatory James R. Stellar, Senior Vice President for Academic Affairs and Provost	518.956.8030

[5] The NY State Education Department reserves the right to request this data at any time and to use such data as part of its evaluation of future program registration applications submitted by the institution.

Section 2. Program Information

2.1. Program Format

Check all SED-defined formats, mode and other program features that apply to the **entire program**.

a) Format(s): [X]Day [ ]Evening [ ]Weekend [ ]Evening/Weekend [ ]Not Full-Time

b) Modes: [X]Standard [ ]Independent Study [ ]External [ ]Accelerated [ ]Distance Education
NOTE: *If the program is designed to enable students to complete 50% or more of the course requirements through distance education, check Distance Education, see Section 10, and append a Distance Education Format Proposal.*

c) Other: [ ] Bilingual [ ] Language Other Than English [ ] Upper Division [ ] Cooperative [ ] 4.5 year [ ] 5 year

2.2. Related Degree Program

NOTE: *This section is not applicable to a program leading to a graduate degree.*

2.3. Program Description, Purposes and Planning

a) What is the description of the program as it will appear in the institution's catalog?

Program Description

M.S. in Digital Forensics and Cyber Operations is a one year 36-credit intense program that includes 15 credits of coursework during both the fall and spring semesters, and a 6-credit internship/thesis during the summer at the tail end of the program. The program trains students in the field of digital forensics and security analytics. As the nature of cyber security and digital forensics changes from fields driven by government and law enforcement to a critical capability for all companies, both large and small, there is a great need for individuals to be trained in these fields. The program teaches students advanced technical skills in digital data processing and analytics as well as domain knowledge in information security and digital forensics. Students can specialize in one of three tracks i.e. cyber defense, digital forensics, and cyber operations. The cyber defense track prepares students in cyber incident investigation with a strong component of security data analysis; the digital forensics track prepares students for the collection, preservation and analysis of data found in electronic devices; and the cyber operations track teaches students proactive threat hunting and offensive/defensive operations. The program concludes with a 6-credit internship/thesis in the summer following two semesters of coursework; students pick their choice based on their career goals (e.g. intelligence, risk advisory, e-discovery, corporate or public sector cybersecurity, law enforcement, or higher education).

Requirements for Admission

In addition to the general University requirements for admission to graduate studies, an applicant's undergraduate major preferably should have been in Cyber Security, Digital Forensics, Computer Science, or Information Science. Students who are deficient in their basic skills of networking, databases, Python programming, cyber security and operating systems, must make up such deficiencies before being formally admitted into the program. Students wishing to enter the program must have a 3.2 grade point average in their undergraduate studies, a Graduate Readiness Examination (GRE) score of 700, or a Graduate Management Admission Test (GMAT) score of 580. International Students will be required to score a 100 on the Test of English as a Foreign Language (TOEFL).

Program Requirements

- Full time students wishing to graduate in one year be required to enroll in five classes per semester.
- Students will have to select one of three specializations upon acceptance into the program (Cyber Defense, Cyber Operation, or Digital Forensics)
- The digital forensics and cyber defense specializations will require four core courses and one elective course in each semester and the cyber operations track will have four required courses and one elective in the fall, and three required courses and two elective courses in the spring.
- Students will have to complete a 6-credit thesis/internship anytime during the regular academic year or the following summer. The thesis/internship will be S/U graded. Students opting for the thesis option, will identify an advisor at the beginning of the Spring semester and finish their problem statement and literature review during the spring semester and then conduct their research and thesis writeup over the summer.
- Students are expected to have basic knowledge of programming, networking, and information security before they begin their studies

b) What are the program's educational and, if appropriate, career objectives, and the program's primary student learning outcomes (SLOs)? ***NOTE:*** *SLOs are defined by the Middle States Commission on Higher Education in the Characteristics of Excellence in Higher Education (2006) as "clearly articulated written statements, expressed in observable terms, of key learning outcomes: the knowledge, skills and competencies that students are expected to exhibit upon completion of the program."*

Program Description
The program will provide students with the skillset to address the challenges in protecting data on and collecting data from information systems, the law and ethics surrounding cybersecurity and digital forensics, as well as the protection of cyber systems from attacks. Upon successful completion of the program, graduates will be attractive to recruiters from intelligence agencies, law enforcement, and the private / industry sector as analysts, consultants, investigators and security analysts. Additionally, this program will provide professional education for adult learners already working in similar fields or looking to enter the information security or digital forensics fields.

The Learning Objectives of the Students are:

General:

- Students will have competencies in programming and data analytics that they can leverage in the specialization courses
- Students will learn domain knowledge in the area of cyber security and digital forensics that will be the foundation for more advanced courses
- Students will learn critical thinking and problem-solving skills when faced with technical challenges

Digital Forensics Track

- Students gain knowledge of:
    - Computer and Forensic hardware systems
    - Current standards and quality management for forensic operations
    - Common operating systems and file formats
    - Mobile Devices
    - Supervisory Control and Data Acquisition Systems
    - Internet of Things Systems
    - Memory collection and preservation techniques
    - Data analysis
    - Programming
    - Forensic tool testing and validation
    - Common cyber security threats
- The skills that students will obtain in this program are:
    - The use of forensic tools that are commonly used in the field and in labs by forensic practitioners
    - The investigation of a digital device or a physical scene in pursuit of evidence
    - Writing comprehensive reports and other documentation associated with forensic investigations
    - Disseminating findings in a testimonial format
    - The development of standards for forensic investigations
    - Implementing a quality management system for field and lab operations
    - Data and memory preservation techniques
- Students will demonstrate the following abilities:
    - Extract data from common digital devices
    - Analyze extracted data for items of interest to an investigation
    - Apply current standards to their digital investigations
    - Conduct technical reviews of analysis findings to ensure quality
    - Convey findings in written and oral formats
    - Prove that the results of an investigation are forensically accurate
    - Sanitize data retrieved from hardware to ensure privacy protection
    - Gain information from a dataset through analytics
    - Determine the threats a system faces and how to defend against them

Cyber Defense Track

- Students will obtain a knowledge of:
    - Data analysis
    - Programming for analytics
    - Cyber security threats and controls

- Computer forensics
- Risks to information systems
- Computer hardware and operating systems
- Malware reverse engineering
- Anomaly/Intrusion Detection and Incident Response
- How Machine Learning and Artificial Intelligence can be used in cyber defense

- The skills that students will obtain in this program are:
  - Risk Analysis
  - Leveraging standards and frameworks to develop security policies
  - Applcation of analytics to cybersecurity
  - Network monitoring, vulnerability scanning, and network mapping tools

- Students will demonstrate the following abilities
  - Development of organizational security polices to show regulatory compliance
  - Analyze and manage risks for an organization
  - Setup a network monitoring system and analyze the traffic on network
  - Analyze a cybersecurity incident
  - Determine the threats a system faces and how to defend against them
  - Sanitize data retrieved from hardware
  - Gain information from a dataset through analytics

Cyber Operations Track

- Students will obtain a knowledge of:
  - Low Level Programming
  - Reverse Engineering
  - Discrete Mathematical Logic and Algorithms
  - Information/Cybersecurity
  - Laws and Ethics for cyber security and cyber operations
  - SCADA System Security
  - Penetration Testing
  - Threats and threat actors
  - Open source intelligence (OSINT)
- The skills that students will obtain in this program are:
  - Threat Analysis
  - Identification of malicious code/activities
  - Interpreting international and US Law
  - Security techniques, architecture and components (e.g., firewalls, IDS, etc.)
  - Programming and securing SCADA systems
  - Symmetric and asymmetric cryptography, integrity, digital signatures, and key management
  - Vulnerability idendifcation
  - Threat mitigation
  - Mission planning and execution process
  - Identifaction of threats and threat actors
  - Identification of open source intelligence gathering techniques and sources
- Students in this track will demonstrate the following abilities:
  - Probe information systems to test their defenses
  - Understand and apply cyber laws and ethics
  - Secure embedded/SCADA systems from unauthorized access
  - Apply cryptographic protocols to their communications
  - Design and test algorithms
  - Identify and mitigate threats
  - Describe the motivations for various threat actors
  - Use Linux operating system to attack other operating systems
  - Use open source intelligence to gather information on a target

b) How does the program relate to the institution's and SUNY's mission and strategic goals and priorities? What is the program's importance to the institution, and its relationship to existing and/or projected programs and its expected impact on them? As applicable, how does the program reflect diversity and/or international perspectives? For doctoral programs, what is this program's potential to achieve national and/or international prominence and distinction?

How does the program relate to the institution's and SUNY's mission and strategic goals and priorities?

The program will fulfill several objectives from the 2017 Strategic Plan, mainly in terms of imperative 2 "Innovate Programs to Meet 21st Century Societal Challenges" strategic initiative 2.1 "Foster an environment that promotes dynamic academic innovation across the boundaries of today's disciplines, departments and colleges. Engage the faculty in defining the mix of programs, particularly at the master's and doctoral levels, that will enable UAlbany to develop a competitive advantage, to better articulate the contemporary role of the arts and humanities, and to enhance our identity as a public research university."

Many new technology innovations, like self-driving cars, a smart electric grid, or implantable electronic medical devices, leverage information systems and networks to improve quality of life. These innovations impact critical infrastructure and the human body by adding intelligence and ability for autonomous behavior. Society's increasing dependence on autonomous systems in critical functions creates the risk that anomalies or cyberattacks on these systems could lead to large-scale, catastrophic failures and loss of life. With greater system complexity comes decreased visibility, which limits our ability to detect and correct anomalies or thwart attacks. Forensic analysts and cyber security experts must gain visibility into these networks so they can rapidly detect and address anomalies and attacks. As we increasingly adopt these technologies, we will have needs for forensics/security experts who can decipher the data and identify these anomalies and attacks. If an accident involves a self-driving car, who is at fault? A forensic examiner will have to analyze crash data to identify failures and establish culpability for law enforcement or insurers. Our program will produce experts who can address these issues – the market for such talent is growing and the growth will only accelerate as these technologies make deeper penetration into society.

What is the program's importance to the institution, and its relationship to existing and/or projected programs and its expected impact on them?

The program directly impacts a key driver for the University by growing graduate enrollment. We anticipate strong enrollments from the University (College of Emergency Preparedness, Homeland Security, and Cyber Security, College of Engineering and Applied Sciences) and our Undergraduate Program in Digital Forensics. We will also get good placement from students from outside given the strong reputation of our undergraduate program and the unique and innovative design of the program that targets a growth market. Additionally, the 1 year program and evening classes affords an opportunity to working professionals in technology related fields that meet the program admission requirements further increase enrollment.

As applicable, how does the program reflect diversity and/or international perspectives? For doctoral programs

Our undergraduate program, created four years ago, has strong diversity with 35% women and minorities in the program. We expect to have similar demographics for our master's program based on our recruiting pool. Given the nature of the field and the short duration of the program, we believe that this program will be very attractive to international students. We are currently establishing relationships with universities in other countries to create a pipeline of international students into our program.

What is this program's potential to achieve national and/or international prominence and distinction?

Students from this program will have a strong placement and we will be able to recruit top students. Our undergraduate program is 4 years old and already has a national reputation we expect this to become one of the top programs internationally in a very short duration (3-5 years).

d) How were faculty involved in the program's design? Describe input by external partners, if any (e.g., employers and institutions offering further education?

We have had regular meetings to discuss the curriculum in 2016-2017; the faculty has been instrumental in designing the courses that we need for the program collectively. We have presented this to our advisory board and incorporated their feedback into the program. Based on discussions with industry and review of NSA accreditation guidelines, we decided both on the length of the program (1-year) and the three tracks that we have in the program.

e) How did input, if any, from external partners (e.g., educational institutions and employers) or standards influence the program's design? If the program is designed to meet specialized accreditation or other external standards, such as the educational requirements in Commissioner's Regulations for the profession, append a side-by-side chart to show how the program's components meet those external standards. If SED's Office of the Professions requires a specialized form for the profession to which the proposed program leads, append a completed form at the end of this document.

As discussed above, the program was evaluated by our advisory board as well as faculty in two different institutions with strong security and forensics programs. These business professionals and well-regarded faculty gave suggestions which have been incorporated in the design of the program. The cyber advisory board consists of:

- Sanjay Goel, Chair, Program Director Digital Forensics Program / Graduate Certificate in Information Security
- George Hickman, Chief Information Officer, Albany Medical Center

- Joel Ryba, Chief Executive Officer, XchangeWorx, Inc.
- Deborah Snyder, Chief Information Security Officer, NYS Office of Information Technology Services
- Bernard Hillengas, Vice President of Business Solutions, Rational Enterprise
- Reg Harnish, Chief Executive Officer, GreyCastle Security
- Martin Manjak, Chief Information Security Officer, Information Technology Services, UAlbany
- Matt Ammerman, Global Client CTO, Apprenda
- Steven Spano, President & COO, Center for Internet Security
- Brian DePersiis, Senior Manager, Advisory Services, Ernst & Young LLP
- Rob Zeglen, Information Security Practice Leader, New York State Technology Enterprise Corporation (NYSTEC)
- Teresa Zielinski, SVP, Global CISO & Product Security, GE Power
- Matt Anglin, ISO, New York State Information Services Operator
- Chris Horn, ISO, Secure Decisions
- Kevin Reedy, ISO, MM Hayes
- Aileen Judd, ex-NSA

f) Enter anticipated enrollments for Years 1 through 5 in the table below.

These projections were based on consultation from projected employers, discussions with current undergraduates enrolled in the Digital forensics program at Albany and discussions with other universities offering a Digital Forensics and Cybersecurity MS. We fully expect to meet the projected targets since a lot of the demand is from our undergraduate students, however, we have contingency plans for boosting our enrollment by crafting a Graduate Certificate in Digital Forensics that will complement our Graduate Certificate in Information Security. This will be a 5-course sequence that will completely overlap with the courses of the MS program. We will also be able to tap into part-time students from NYS State and other industries around the area.

Year	Anticipated Headcount Enrollment			Estimated FTE
	Full-time	Part-time	Total	
1	16		16	
2	20		20	
3	24		24	
4	30		30	
5	32		32	

Here are enrollments at John Jay the past few years, a school with and enrollment that is 13% smaller than Albany's and lacks a digital forensics only bachelors program. Given that we have a much larger base of students to select from we are fairly confident we will be able to meet our enrollment targets.

Program	F12	F13	F14	F15	F16
MS Digital Forensics & Cybersecurity	18	18	14	17	18
Applied Digital Forensic Science	NA	NA	0	0	1
Computer Science for Digital Forensics	0	5	7	8	5

g) Outline all curricular requirements for the proposed program, including prerequisite, core, specialization (track, concentration), internship, capstone, and any other relevant component requirements, but do not list each General Education course.

FORENSICS TRACK

	FALL		SPRING	
	Course Number & Title	CR	**Course Number & Title**	CR
Core	BFOR 516 Advanced Data Analysis	3	BFOR 620 Digital Forensics Lab Mgt.	3
	BFOR 511 System Admin & OS Concepts	3	BFOR 607 Memory Forensics & Analysis	3
	BITM 644 Cyber Threats and Defense	3	BFOR 604 Mobile Forensics	3
	BITM 642 Computer Forensics	3	BFOR 613 Multimedia Forensics	3
Elective	BFOR 520 Open Source Intel. & Social Net. Anal	3	B3FOR 611 SCADA Security & Forensics	3
	BFOR 506 Database Security & Forensics	3	BFOR 622 Cloud Security & Forensics	3
			BFOR 602 Cyberlaw & Ethics	3
			BITM 643 Cyber Incident Analysis	3
	TOTAL	15	TOTAL	15

CYBER DEFENSE TRACK

	FALL		SPRING	
	Course Number & Title	CR	**Course Number & Title**	CR
Core	BFOR 516 Advanced Data Analysis	3	BITM 640 Inf. Security Analysis	3
	BFOR 511 System Admin & OS Concepts	3	BITM 643 Cyber Incident Analysis	3
	BITM 644 Cyber Threats and Defense	3	BFOR 647 Security Implementation	3
	BITM 642 Computer Forensics	3	BFOR 615 Hacking for Pen Testing	3
Elective	BFOR 520 Open Source Intel. & Social Net. Anal	3	B3FOR 611 SCADA Security & Forensics	3
	BFOR 506: Database Security & Forensics	3	BFOR 622 Cloud Security & Forensics	3
			BFOR 602 Cyberlaw & Ethics	3
			BITM 643 Cyber Incident Analysis	3
	TOTAL	15	TOTAL	15

CYBER OPERATIONS TRACK

	FALL		SPRING	
	Course Number & Title	CR	**Course Number & Title**	CR
Core	BFOR 525 Advanced Networking	3	BFOR 632 Cyber Threat Hunting	3
	BITM 644 Cyber Threats & Defense	3	BFOR 650 SCADA Vul. Exploitation	3
	BFOR 618 Reverse Engineering Malware	3	BFOR 602 Cyberlaw & Ethics	3
	BFOR 646 Math. Models for Info. Security	3		
Elective	BFOR 520 Open Source Intel. & Social Net. Anal	3	BFOR 610 International Cyber Conflicts	3
	BFOR 611 SCADA Security & Forensics	3	BFOR 615 Hacking for Pen Testing	3
			BFOR 607 Memory Forensics & Analysis	3
			BFOR 613 Multimedia Forensics	3
	TOTAL	15	TOTAL	15

THESIS/INTERNSHIP

	SUMMER	
	Course Number & Title	CR
	BFOR 525 Advanced Networking	3
	TOTAL	15

h) Program Impact on SUNY and New York State

h) (1) ***Need:*** What is the need for the proposed program in terms of the clientele it will serve and the educational and/or economic needs of the area and New York State? How was need determined? Why are similar programs, if any, not meeting the need?

While information security education has grown significantly over the past 10 years, education in Digital Forensics, Cyber Incident Analysis, and Cyber Operations have only recently emerged as critical specialty in the information security domain. Digital Forensics is a branch of forensic science that involves investigation, recovery, an analysis of information from digital devices. These devices can include computers, smartphones, smart appliances, digital cameras, etc. Cyber Defense deals with protection of computers and networks as compared to Digital Forensics deals with live and post-mortem analysis of computer attacks, fraud and other traditional computer-related investigations; collection and presentation of digital evidence; and determinations of responsibility and consequences. Cyber Incident Analysis involves detection of intrusions and attacks as well as responding to incidents to mitigate the damage and prevent future attacks. Cyber Operations involves active threat hunting from our adversaries (e.g. nation states, terrorist organizations, and organized crime syndicates) and includes both defensive and offensive operations. All of these activities have obvious benefits to the community-at-large by providing the capabilities and workforce to fill the demand for professionals to ensure the security and safety of citizens and the preservation of justice.

The National Academies of Science have cautioned that the people of the United States will face a lower standard of living if knowledge-intensive jobs further decline in the US.[1] American workers face increased job competition from lower-wage workers internationally, with leading-edge scientific and technology jobs being performed in many parts of the world. Consequently, large numbers of students are moving away from STEM fields including computing and engineering[2]. To increase enrollments in these fields, Denning and McGettrick[3] have suggested reengineering traditional computing education to focus on specialized fields. As enrollments drop in technology-based disciplines, new programs are emerging in specialized fields, such as Digital Forensics, to attract students disenfranchised by traditional computing. **In the past, demand for professionals in this field primarily came from law enforcement agencies[4]; today, the demand is largely coming from private-sector organizations and is being driven by business needs including: data recovery, electronic discovery, incident response, policy auditing and third-party forensic analysis services[5].** Today the demand for Digital Forensics is in investigating intrusions in networks through logging and analysis of data on networks. According to the Bureau of Labor Statistics, demand for in forensic science technicians is expected to grow by17% by 2026[6]. Additionally, the demand for Certified Information Security Systems Professionals is currently outpacing supply[7]. Creating a Digital Forensics and Cyper Operations program is a natural next step that builds on our past successes in the area of information security and will place UAlbany at the forefront in this area.

The demand for Digital Forensics, Cyber Defense and Cyber Operations training is outpacing supply – leading to an acute shortage of trained professionals nationally and internationally. The need for Digital Forensics education has grown as use of computers in crime and fraud has become a significant threat in the United States but around the world. According to Norton Cybercrime Report 2011[8], net cybercrime costs globally equal $388 billion across 24 countries – more than the black markets for marijuana, cocaine, and heroin combined ($288 billion) and close to the value of the total global drug trafficking market ($488 billion). New York State is innovating rapidly and the innovations leveraging information technology will stall if talent is not available. Businesses are increasingly being targeted by international crime rings through the Internet and we need to train the workforce that can defend against these attacks. In 2016 there were 1 million cyber security jobs and they are expected to grow to 3.5 million by 2021. We need to put the seeds in place now and build capacity now before businesses start moving overseas in search of new talent.

h) (2) ***Employment:*** For programs designed to prepare graduates for immediate employment, use the table below to list potential employers of graduates that have requested establishment of the program and state their specific number of positions needed. If letters from employers support the program, they may be **appended** at the end of this form.

Employer	*Need: Projected positions*	
	In initial year	In fifth year
New York State Information Technology Services	2-3	5-7
Center for Internet Security	1-2	3-5
EY	2-3	5-7
General Electric	2-3	5-7
Rational Enterprises	1-2	2-3
Albany Medical Center	1-2	3-4

[1] National Academies of Science (NAS). Committee on Science, Engineering, and Public Policy. (2007). *Rising above the gathering storm: energizing and employing America for a brighter economic future.* Washington, DC, USA: The National Academies Press.
[2] Seymour, E. & Hewitt, N. M. (2000). *Talking about leaving: why undergraduates leave the sciences.* Boulder, CO, USA: Westview Press.
[3] Denning, P. J. & McGettrick, A. (2005, November). Recentering computer science. Communications of the ACM, 48(11), 15-19.
[4] Yasinsac, A., Erbacher, R. F., Marks, D. G., Pollitt, M. M., Sommer, P. M. (2003). Computer forensics education. IEEE *Security & Privacy, 2003*(1), 15–23.
[5] Kessler, G. C. & Haggerty, D. A. (2010). An online graduate program in digital investigation management: pedagogy and overview. *Journal of. Digital Forensic Practice 3*(1), 11-22.
[6] United States. Department of Labor. Bureau of Labor Statistics.(2016). *Occupational Outlook Handbook, 2016 Edition.*
[7] Vijayan, J. (2013). Demand for it security experts outstrips supply. https://www.computerworld.com/article/2495985/it-careers/demand-for-it-security-experts-outstrips-supply.html
[8] Symantec. (2011). Norton Cyber Crime Report 2011. Retrieved from: http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/

Deloitte	2-3	5-7
PWC	2-3	5-7

h) (3) ***Similar Programs:*** Use the table below to list similar programs at other institutions, public and independent, in the service area, region and state, as appropriate. Expand the table as needed. ***NOTE:*** *Detailed program-level information for SUNY institutions is available in the Academic Program Enterprise System (APES) or Academic Program Dashboards. Institutional research and information security officers at your campus should be able to help provide access to these password-protected sites. For non-SUNY programs, program titles and degree information – but no enrollment data – is available from SED's Inventory of Registered Programs.*

Institution	Program Title	Degree	Enrollment
Utica College	M.S. Cyber Security	M.S.	
John Jay Col. of Criminal	M.S. Digital Forensics	M.S.	

h) (4) ***Collaboration:*** Did this program's design benefit from consultation with other SUNY campuses? If so, what was that consultation and its result?

This program has a unique focus (security analytics and forensics), which makes it quite different from other MS programs in the SUNY system. We have had discussions about the program with John Jay College of Criminal Justice.

h) (5) ***Concerns or Objections:*** If concerns and/or objections were raised by other SUNY campuses, how were they resolved?

No objections have been raised by other campuses we have discussed with, during the letter of intent period.

2.4. Admissions

a) What are all admission requirements for students in this program? Please note those that differ from the institution's minimum admissions requirements and explain why they differ.

The admissions requirements for the MS in Digital Forensics and Cyber Security include (1) evidence of academic achievement (transcripts, letters of recommendation) and (2) evidence of overall graduate education preparedness and capability (GRE/GMAT, TOEFL). The student entering the program must have completed their GRE/GMAT exam as well as completed their undergraduate degree in computer science, digital forensics, computer security, information science, informatics departments. Students should submit two letters of references as a testament to the ability of the student as well as a written essay outlying the student's interest in the field and how their previous education and experience prepared them to study in the program. This is a competitive program with limited seats and the most qualified students will be admitted to the program based on the GPA, GRE/GMAT scores, letters of references, and personal essay. Students must demonstrate readiness for the program's rigor by having a 3.2 grade point average in their undergraduate studies, a Graduate Readiness Examination (GRE) score of 700, or a Graduate Management Admission Test (GMAT) score of 580. International Students will be required to score a 100 on the Test of English as a Foreign Language (TOEFL).

b) What is the process for evaluating exceptions to those requirements?

Evaluating exceptions to these requirements will be done by interviews of these students with the program director and relevant faculty members. Additionally, a voluntary practicum or hands-on workshop may be offered to a student prior to admission that affords the student an opportunity to refresh their technical, critical thinking and writing skills.

c) How will the institution encourage enrollment in this program by persons from groups historically underrepresented in the institution, discipline or occupation?

The reference for the demographics for digital forensics is the field of computer science. In computer science the gender disparity is severe, with only 18% of degrees being conferred to women[9]. Some 61% of students are Caucasian, about 8-11% are African-American, Asian/Pacific Islander or Other/Unknown, 3.3% are Hispanic, and 0% are Native American/Alaskan. The trend in our Digital Forensics Undergraduate Major is quite different with about 35% females in the program. We have a large number of female faculty in the program to which makes the environment more supportive for women, and provides ready access to potential female role models and mentors. For minority recruitment, we work closely with the Office of Access and Academic Enrichment (AAE) which oversees the campus Science & Technology Entry Program (STEP) and Collegiate Science & Technology Entry Program (CSTEP). AAE will assist in recruiting undergraduate students at UAlbany in underrepresented populations.

d) What is the expected student body in terms of geographic origins (i.e., same county, same Regents Region, New York State, and out-of-state); academic origins; proportions of women and minority group members; and students for whom English is a second language?

We expect to have about 70% of students from New York State, many of whom will come from our undergraduate programs in Digital Forensics, Computer Science, Informatics, and Homeland Security. We expect about 20% students from out of state who will be attracted by the uniqueness and reputation of the program and 10% international students from the pipelines that we have built across different countries. About 20-25% of our population may be from students who have English as their second language.

2.5. Academic and Other Support Services

a) Summarize the academic advising and support services available to help students succeed in the program.

M.S. in Digital Forensics & Cyber Security students will be advised by the well-established School of Business Office of Graduate Student Services, which has been functioning as the main advisement center for 40 years. Additionally, all students in this program will be encouraged to select a faculty mentor to discuss appropriate elective courses, as well as, various career opportunities and advance study in this field.

b) Describe types, amounts and sources of student financial support anticipated. Indicate the proportion of the student body receiving each type of support, including those receiving no support.

The students in this program will be primarily self-funded. We will seek out additional funding to help defray costs for students. Some students may be supported by scholarships from private sources, foundations or agencies.

2.6. Prior Learning Assessment

If this program will grant credit based on Prior Learning Assessment, describe the methods of evaluating the learning and the maximum number of credits allowed, **or check here [X] if not applicable**.

[9] http://newsroom.ucla.edu/stories/cracking-the-code:-why-aren-t-more-women-majoring-in-computer-science

2.7. Program Assessment and Improvement

Describe how this program's achievement of its objectives will be assessed, in accordance with *SUNY policy*, including the date of the program's initial assessment and the length (in years) of the assessment cycle. Explain plans for assessing achievement of students learning outcomes during the program and success after completion of the program. **Append** at the end of this form, **a plan or curriculum map** showing the courses in which the program's educational and, if appropriate, career objectives – from Item 2.3(b) of this form – will be taught and assessed. ***NOTE:*** *The University Faculty Senate's Guide for the Evaluation of Undergraduate Programs is a helpful reference.*

The program's assessment will comply the same format as other graduate programs in the School of Business. Consistent with University policy, the School of Business maintains a 7-year assessment cycle for its programs. The program faculty will apply the same methodology to the assessment of the MS in Digital Forensics & Cyber Security that it performs in the assessment of all its programs. This will include direct assessment of student work in core courses, indirect assessment through student surveys, and indirect assessment through student focus groups. The assessment methods will identify successes and deficiencies in the program, and faculty will use the assessment results to address deficiencies and build and maintain program strength. As part of the 7-year assessment cycle, the program faculty will conduct yearly assessments of its programs and courses to determine whether learning objectives are being met. Assessments at this level are conducted through specific assignments and item analyses of examination responses to questions related to targeted learning objectives.

In addition, to this mandatory assessment in 7-year we will conduct an informal review and assessment half-way through the University mandated assessment cycle. This will primarily be done to align our programs with the standards defined by NSA/NIST for ensuring relevance in the work place. Additionally, this will support re-accreditation with the NSA Center of Academic Excellence status for the program. The program will be mapped to national standards; post placement employer surveys will be conduncted to gauge the how well our students meet the needs if their employers, and the assessment/critique of the advisory board will be solicited to update the curriculum. We will also survey graduates with respect to the relevance and use of knowledge, skills and competencies acquired in the M.S. program.

Section 3. Program Schedule and Curriculum

Complete the **SUNY Graduate Program Schedule** to show how a typical student may progress through the program. This is the registered curriculum, so please be precise. Enter required courses where applicable and enter generic course types for electives or options. Either complete the blank Schedule that appears in this section, or complete an Excel equivalent that computes all sums for you, found here. Rows for terms that are not required can be deleted.

NOTES: *The* ***Graduate Schedule*** *must include all curriculum requirements and demonstrate that expectations from in Regulation 52.2 http://www.highered.nysed.gov/ocue/lrp/rules.htm are met.*

Special Cases for the Program Schedules:

- ☐ *For a program with multiple tracks, or with multiple schedule options (such as full-time and part-time options), use one Program Schedule for each track or schedule option. Note that licensure qualifying and non-licensure qualifying options cannot be tracks; they must be separate programs.*
- ☐ *When this form is used for a multi-award and/or multi-institution program that is not based entirely on existing programs, use the schedule to show how a sample student can complete the proposed program.* ***NOTE:*** *Form 3A, Changes to an Existing Program, should be used for new multi-award and/or multi-institution programs that are based entirely on existing programs. SUNY policy governs the awarding of two degrees at the same level.*

a) If the program will be offered through a nontraditional schedule (i.e., not on a semester calendar), what is the schedule and how does it impact financial aid eligibility? ***NOTE:*** *Consult with your campus financial aid administrator for information about nontraditional schedules and financial aid eligibility.*

N/A

b) For each existing course that is part of the proposed graduate program, **append** a catalog description at the end of this document.

DONE

c) For each new course in the graduate program, **append** a syllabus at the end of this document. ***NOTE:*** *Syllabi for all courses should be available upon request. Each syllabus should show that all work for credit is graduate level and of the appropriate rigor. Syllabi generally include a course description, prerequisites and corequisites, the number of lecture and/or other contact hours per week, credits allocated (consistent with SUNY policy on credit/contact hours), general course requirements, and expected student learning outcomes.*

DONE

a) If the program requires external instruction, such as clinical or field experience, agency placement, an internship, fieldwork, or cooperative education, **append** a completed External Instruction form at the end of this document

BFOR660 will be the practicum for the students. External Instruction form is attached.

SUNY Graduate Program Schedule (*OPTION: You can insert an Excel version of this schedule AFTER this line and delete the rest of this page.)*

Program/Track Title and Award:_____

a) Indicate **academic calendar** type: [X] Semester [ ] Quarter [ ] Trimester [ ] Other (describe):

b) **Label each term in sequence**, consistent with the institution's academic calendar (e.g., Fall 1, Spring 1, Fall 2)

c) Use the table to show **how a typical student may progress through the program**; copy/expand the table as needed.

d) Complete the last row to show program totals and comprehensive, culminating elements. **Complete all columns that apply to a course.**

FORENSICS TRACK

Term 1:Fall 1			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**
BFOR 516 Advanced Data Analysis (Fan) or BITM 603 Data Analytics in Business	3		
BFOR 511 System Administration & Operating Systems Concepts (Augustine)	3		
BITM 644 Cyber Threats and Defense (M. Smith)	3		
BITM 642 Computer Forensics (Auffant)	3		
Electives			
BFOR 520 Open Source Intel. and Social Network Data Analysis (Majumdar)	3	X	
BFOR 506: Database Security & Forensics (Fan)	3	X	
Term credit total:	15		

Term 2: Spring 1			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**
BFOR 620 Digital Forensics Quality Management Systems (Auffant)	3	X	
BFOR 607 Memory Forensics & Analysis (TBH1)	3	X	
BFOR 604 Mobile Forensics (Gallo)	3	X	
BFOR 613 Multimedia Forensics (Salhoff)	3		
Electives			
BFOR 611 SCADA Security & Forensics (Salhoff)	3		
BFOR 622 Cloud Security & Forensics (Majumdar)	3	X	
BFOR 602 Cyberlaw, & Ethics (TBH2)	3	X	
BITM 643 Cyber Incident Analysis (Manjak)			
Term credit total:	15		

Term 3: (SUMMER)			
Course Number & Title	**Credit**	**New**	**Co/Prerequisite**
BFOR 660 Internship/Thesis	6	X	
Term credit total:	6		

Term 4:			
Course Number & Title	**Credit**	**New**	**Co/Prerequisite**
Term credit total:			

Program Total:	**Total Credits:36**	**Identify the required comprehensive, culminating element(s), such as a thesis or examination, including course number(s), if applicable:** BFOR 660

CYBER DEFENSE TRACK

Term 1: Fall 1			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**
BFOR 516 Advanced Data Analysis (Fan) or BITM 603 Data Analytics in Business	3		
BFOR 511 System Administration & Operating Systems Concepts (Augustine)	3		
BITM 644 Cyber Threats & Defense (Smith)	3		
BITM 642 Computer Forensics (Auffant)	3		
Electives			
BFOR 520 Open Source Intelligence & Social Network Data Analysis (Majumdar)	3	X	
BFOR 506: Database Security & Forensics (Fan)	3	X	
Term credit total:	15		

Term 2: Spring 1			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**
BITM 640 Information Security Risk Analysis (Snyder)	3		
BITM 643 Cyber Incident Analysis (Manjak)	3		
BFOR 647 Security Implementation (Smith)	3		
BFOR 615 Hacking for Pen Testing (TBH2)	3	X	
Electives			
BFOR 645 Psychology & Information Security (Williams)	3		
BFOR 610 International Cyber Conflicts (Goel)	3		
BFOR 622 Cloud Security & Forensics (Majumdar)	3	X	
Term credit total:	15		

Term 3: (SUMMER)			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**
BFOR 660 Internship/Thesis	6	X	
Term credit total:			

Term 4:			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**
Term credit total:			

Program Total:	**Total Credits:36**	**Identify the required comprehensive, culminating element(s), such as a thesis or examination, including course number(s), if applicable: BFOR 660**

CYBER OPERATIONS TRACK

Term 1: Fall 1				**Term 2: Spring 1**			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**	**Course Number & Title**	**Credits**	**New**	**Co/Prerequisites**
BFOR 525 Advanced Networking (TBH2)	3	X		BFOR 632 Cyber Threat Hunting (Goel)	3	X	
BITM 644 Cyber Threats & Defense (Smith)	3			BFOR 650 SCADA Vulnerability Exploitation (TBH1)	3	X	
BFOR 618 Reverse Engineering Malware (Majumdar)	3	X		BFOR 602 Cyberlaw & Ethics (TBH2)	3	X	
BFOR 646 Mathematical Models for Information Security (Bhattacharya)	3				3	X	
Electives				**Electives**			
Course Number & Title	**Credits**	**New**	**Co/Prerequisites**	**Course Number & Title**	**Credits**	**New**	**Co/Prerequisites**
BFOR 520 Open Source Intelligence & Social Network Data Analysis (Majumdar)		X		BFOR 610 International Cyber Conflicts (Goel)	3		
BFOR 611 SCADA Security & Forensics (Salhoff)				BFOR 615 Hacking for Pen Testing (TBH2)	3	X	
				BFOR 607 Memory Forensics & Analysis (TBH1)		X	
Term credit total:	15			Term credit total:	15		
Summer:							
BFOR 660 Internship/Thesis	6	X					
Term credit total:	6			Term credit total:			
Program Total:	**Total Credits:36**			**Identify the required comprehensive, culminating element(s), such as a thesis or examination, including course number(s), if applicable:** BFOR 660			

Section 4. Faculty

a) Complete the **SUNY Faculty Table** on the next page to describe current faculty and to-be-hired (TBH) faculty.

b) **Append** at the end of this document position descriptions or announcements for each to-be-hired faculty member.

NOTE: *CVs for all faculty should be available upon request. Faculty CVs should include rank and employment status, educational and employment background, professional affiliations and activities, important awards and recognition, publications (noting refereed journal articles), and brief descriptions of research and other externally funded projects. New York State's requirements for faculty qualifications are in in Regulation 52.2* http://www.highered.nysed.gov/ocue/lrp/rules.htm

c) What is the institution's definition of "full-time" faculty?

A full-time faculty member at the University at Albany is an individual employed in a faculty line in a full-time capacity. A typical teaching load for a tenured or tenure-track faculty member in a primarily graduate-focused department is 2 courses each semester, with an additional expectation of research, service, and advising of graduate students and chairing of doctoral dissertations. This load is adjusted for clinical faculty.

SUNY Faculty Table

Provide information on current and prospective faculty members (identifying those at off-campus locations) who will be expected to teach any course in the graduate program. Expand the table as needed. Use a separate Faculty Table for each institution if the program is a multi-institution program.

(a) Faculty Member Name and Title/Rank (Include and identify Program Director with an asterisk)	(b) % of Time Dedicated to This Program	(c) Program Courses Which May Be Taught (Number and Title)	(d) Highest and Other Applicable Earned Degrees (include College or University)	(e) Discipline(s) of Highest and Other Applicable Earned Degrees	(f) Additional Qualifications: List related certifications, licenses and professional experience in field
PART 1. Full-Time Faculty					
Sanjay Goel*	75%	BITM 610, BFOR 660, BFOR 632	Ph.D., RPI	Mechanical Engineering	Director, Forensics Analysis of Complex Energy and Transportation Systems (FACETS), Chair Information Security and Digital Forensics Department
Fabio Auffant	33%	BITM 642, BFOR 620	M.S., Champlain College	Digital Forensics Management	Head of Computer Crime Unit – Computer Forensic Laboratory, NY State Police; Technical Assessor – Computer Forensics - ANSI-ASQ National Accreditation Board (ANAB)
Kevin Williams	5%	BITM 645	Ph.D., University of South Carolina	Psychology	
Liyue Fan	50%	BFOR 506, BFOR 516	Ph.D. Emory University	Computer Science & Informatics	
Surydipta Majumdar	50%	BFOR 622, BFOR 618, BFOR 520	Ph.D. Concordia University	Information Systems & Engineering	
Devipsita Bhattacharya	25%	BFOR 646	Ph.D. University of Arizona	Management Information Systems	
Part 2. Part-Time Faculty					
Michael Smith	33%	BITM 644, BFOR 647	M.S., James Madison University	Computer Science with Information Security Concentration	Lead Technical Architect, Cyber Readiness and Response Symantec
Deborah Snyder	16%	BITM 640	M.B.A., University at Albany	Business Administration concentration in Cybersecurity	Chief Information Security Officer, New York State Information Technology Services CISSP, CRISC, PMP
Kevin Salhoff	16%	BFOR 613	M.S., Computer Forensics Online Program, Keensaw State University B.S., Rensselaer Polytechnic Institute	Computer Forensics Computer Systems Engineering	Computer Forensic Analyst IV – New York State Police, AccessData Certified Examiner, EnCase Certified Examiner, Certified Cellebrite UFED Physical Examiner, Certified Cellebrite UFED Mobile Device Examiner, Forensic Explorer Examiner, Certified Blacklight Examiner
John Gallo	16%	BFOR 604	A.A.S., Hudson Valley Community College	Criminal Justice	Acting Senior Investigator, New York State Police, Cellebrite UFED Physical/Logical Certified, Access Data Certified Examiner,

					Encase Certified Examiner, Level III Cellular Master Technician
Michael Manjak	16%	BITM 643	B.A., University at Buffalo	Theatre Arts	Chief Information Security Officer, University at Albany, CISSP
William Augustine	16%	BFOR 511	M.S., M.B.A., University at Albany	Computer Science, Information Technology Management	Unix System Administrator, Department of Computer Science, University at Albany
Part 3. Faculty To-Be-Hired (List as TBH1, TBH2, etc., and provide title/rank and expected hiring date)					
TBH1 (full-time, tenure track) – Fall 2019	75%	BFOR 611, BFOR 607, BFOR 650			The hire would teach 25% in the undergraduate program to replace faculty moved from undergraduate to graduate program
TBH2 (full-time, tenure track) -Fall 2019	75%	BFOR 525, BFOR 615, BFOR 602			The hire would teach 25% in the undergraduate program to replace faculty moved from undergraduate to graduate program

Section 5. Financial Resources and Instructional Facilities

a) What is the resource plan for ensuring the success of the proposed program over time? Summarize the instructional facilities and equipment committed to ensure the success of the program. Please explain new and/or reallocated resources over the first five years for operations, including faculty and other personnel, the library, equipment, laboratories, and supplies. Also include resources for capital projects and other expenses.

New instructional facilities are not needed for the program because virtually all of the courses will be taught in existing classrooms in the Business Building at UAlbany. The Massry Center for Business at the University at Albany was constructed in 2013, obtained LEED Gold Certification from the United States Green Building Council. The building contains a stock trading room with Bloomberg Terminals, three cybersecurity laboratories, a host of break out rooms for students to gather in for collaborative work and high-tech classrooms for student instruction. There will be minimal need for additional teaching lab facilities distinct from those used for the existing undergraduate major in digital forensics. State-of-the-art labs exist and can accommodate master's instruction without interfering with undergraduate instruction. To support the existing B.S. in digital forensics, the University Libraries have already expanded their journal collections in digital forensics and related fields.

Graduate student research is funded through grants and faculty start-up funding, including equipment purchases. All faculty are provided laboratory space for their work in addition to start-up funding that can be used to support graduate students, purchase laboratory equipment or software, travel, etc. New laboratories and equipment, therefore, will be added as new faculty are hired and will support the research area(s) and students of these faculty.

b) Complete the five-year SUNY Program Expenses Table, below, consistent with the resource plan summary. Enter the anticipated academic years in the top row of this table. List all resources that will be engaged specifically as a result of the proposed program (e.g., a new faculty position or additional library resources). If they represent a continuing cost, new resources for a given year should be included in the subsequent year(s), with adjustments for inflation or negotiated compensation. Include explanatory notes as needed.

SUNY Program Expenses Table

Program Expense Categories	Before Start (2019)	Academic Year 1	Academic Year 2	Academic Year 3	Academic Year 4	Academic Year 5
(a) Personnel (faculty and all others)	125,000	125,000	0	0	0	0
(b) Library	0	0	0	0	0	0
(c) Equipment	0	0	0	0	0	0
(d) Laboratories	50,000	0	0	0	0	0
(e) Supplies	5,000	10,000	5,000	5,000	5,000	5,000
(f) Capital Expenses	0	0	0	0	0	0
(g) Other (Specify):	0	0	0	0	0	0
(h) Sum of Rows Above	180,000	130,000	5,000	5,000	5,000	5,000

Section 6. Library Resources

a) Summarize the analysis of library collection resources and needs *for this program* by the collection librarian and program faculty. Include an assessment of existing library resources and accessibility to those resources for students enrolled in the program in all formats, including the institution's implementation of SUNY Connect, the SUNY-wide electronic library program.

The University Libraries collects, houses, and provides access to all types of published materials in support of the research and teaching of the schools, colleges, and academic departments of the University.

Library Collections

The University Libraries are among the top 115 research libraries in the country. The University Library, The Science Library,

and the Dewey Graduate Library contain more than two million volumes and over 2.9 Million microforms. The Libraries provide access to more 75,000 online journals and over 117,000 online books. Whenever possible, current subscriptions are available online. Additionally, the Libraries serve as selective depository for U.S. Government publications and houses collections of software and media. The Science Library, which opened in September 1999, occupies 61,124 square feet on four floors. The Science Library serves the entire University at Albany community, but contains collections supporting the departments of Atmospheric and Environmental Sciences, Biological Sciences, Chemistry, Computer Science, Mathematics and Statistics, Physics, Psychology, Electrical and Computer Engineering, and the College of Nanoscale Science and Engineering. Approximately 600,000 volumes in the science and technology subject areas (Q-TP of the Library of Congress classification scheme) are housed in this library. Online resources (journals, databases, e-books, digital libraries) are available on and off campus, all hours of the day.

Books

Currently, it is estimated that there are over 9,000 books in those portions of the Library of Congress (LC) classification scheme which relate to digital forensics, information security, and cybersecurity. Additional printed materials exist on more niche subject such as cyber risk, accounting forensics and cyber-crime in smaller numbers.

Reference Collection

The Science Library reference collection houses many reference resources for computing, computer science, Cybersecurity, information security, and digital forensics. These include guides to the literature, dictionaries, encyclopedias, biographical sources, handbooks, and style guides.

Journals and Magazines

The University Libraries' subscribes to the *ACM (Association for Computing Machinery) Digital Library, IEEE Xplore Digital Library,* Elsevier *(ScienceDirect),* Springer, and Wiley. Furthermore, the University Libraries provide access to many more computing magazines through its subscriptions to full text aggregator databases like *Applied Sciences and Technology Source*, *Computer Source*, *Academic Search Complete*, and *Academic OneFile*. Additionally, two major journals in the field of Digital Forensics, *The Journal of Digital Forensics, Security and Law* and *The International Journal of Digital Forensics & Incident Response* are available by nature of being open source publications and a third the *Journal of Digital Forensic Practice* is available via existing library subscriptions. No additional magazine resources are required.

Databases and Digital Collections

The University Libraries currently subscribes to many databases and digital collections that are important to Digital forensics and cyber security. The databases include, IEEE/IET Electronic Library (IEL), ACM Digital Library, Scopus, INSPEC, SPIE Digital Library, and Springer Computer Science eBook Collection. Those databases are listed and described below. Comprehensive Databases Published by the Institution of Engineering and Technology (IET), INSPEC provides comprehensive indexing of the world's scientific literature for engineering, physics and computer science. It covers journal articles, conference proceedings, reports, dissertations, and books. The *(ACM) Guide to Computing Literature* is a comprehensive database that contains citations from the major English language publishers in computing. Coverage, which dates as far back as 1947, includes books, journal articles, conference proceedings, doctoral dissertations, master's theses, and technical reports. The University Library's subscription to the ACM Digital Library provides cataloging of *The International Journal of Digital Forensics & Incident Response.*

Digital Collections/Full Text Databases

The IEEE Xplore Digital Library is a full-text database that provides access to IEEE journals, transactions, and magazines, including early access documents; IEEE conference proceedings; IET journals, IET conference proceedings, IEEE published standards, IEEE Standards Dictionary Online, etc. It is important to note that IEL contains almost one-third of the world's current literature in electrical engineering, communications, and computer science. The *ACM (Association for Computing Machinery) Digital Library* is a full text database that provides access to all of the association's journals, magazines, special interest group newsletters, and conference proceedings. The *IEEE Computer Society Digital Library* is a full text database that contains the scholarly journals, magazines, and conference proceedings and workshops published by the IEEE Computer Society. *Applied Science and Technology Source* provides access to the full text from more than 1,400 journals and magazines, including scholarly journals, trade magazines, professional society journals, and conference proceedings. Three of the broad subjects covered are engineering, computing, and information technology. Providing access to nearly 300 full text academic journals, magazines, and trade publications, *Computer Source* covers subjects like information systems and robotics. An additional 150 periodicals are also indexed and abstracted.

b) Describe the institution's response to identified collection needs and its plan for library development.

No new collections are anticipated.

Section 7. External Evaluation

SUNY and SED require external evaluation of all proposed graduate degree programs. List below all SUNY- approved evaluators who conducted evaluations (adding rows as needed), and **append at the end of this document** each original, signed *External Evaluation Report.* ***NOTE:*** *To select external evaluators, a campus sends 3-5 proposed evaluators' names, titles and CVs to the assigned SUNY Program Reviewer, expresses its preferences and requests approval.*

Evaluator #1	**Evaluator #2**
Name: John D'Arcy Title: Associate Professor Institution: Delaware University	Name: Nichole Beebe Title: Melvin Lachman Distinguished Professor Institution: University of Texas, San Antonio

Section 8. Institutional Response to External Evaluator Reports

Append at the end of this document a single *Institutional Response* to all *External Evaluation Reports.*

Section 9. SUNY Undergraduate Transfer

NOTE: *SUNY Undergraduate Transfer policy does not apply to graduate programs.*

Section 10. Application for Distance Education

a) Does the program's design enable students to complete 50% or more of the course requirements through distance education? [X] No [] Yes. If yes, **append** a completed *SUNY Distance Education Format Proposal* at the end of this proposal to apply for the program to be registered for the distance education format.

b) Does the program's design enable students to complete 100% of the course requirements through distance education? [X] No [] Yes

Section MPA-1. Need for Master Plan Amendment and/or Degree Authorization

a) Based on guidance on Master Plan Amendments, please indicate if this proposal requires a Master Plan Amendment.
[X] No [ ] Yes, a completed *Master Plan Amendment Form* is **appended** at the end of this proposal.

b) Based on *SUNY Guidance on Degree Authorizations* (below), please indicate if this proposal requires degree authorization.

[X] No [] Yes, once the program is approved by the SUNY Provost, the campus will work with its Campus Reviewer to draft a resolution that the SUNY Chancellor will recommend to the SUNY Board of Trustees.

SUNY Guidance on Degree Authorization. *Degree authorization is required when a proposed program will lead to a new degree (e.g., B.F.A., M.P.H.) at an existing level of study (i.e., associate, baccalaureate, first-professional, master's, and doctoral) in an existing disciplinary area at an institution. Disciplinary areas are defined by the New York State Taxonomy of Academic Programs. Degree authorization requires approval by the SUNY Provost, the SUNY Board of Trustees and the Board of Regents.*

List of Appended Items

Appended Items: Materials required in selected items in Sections 1 through 10 and MPA-1 of this form should be appended after this page, with continued pagination. In the first column of the chart below, please number the appended items, and append them in number order.

Number	Appended Items	Reference Items
	For multi-institution programs, a letter of approval from partner institution(s)	Section 1, Item (e)
	For programs leading to professional licensure, a side-by-side chart showing how the program's components meet the requirements of specialized accreditation, Commissioner's Regulations for the Profession, or other applicable external standards	Section 2.3, Item (e)
	For programs leading to licensure in selected professions for which the SED Office of Professions (OP) requires a specialized form, a completed version of that form	Section 2.3, Item (e)
	OPTIONAL: For programs leading directly to employment, letters of support from employers, if available	Section 2, Item 2.3 (h)(2)
X	*For all programs*, a plan or curriculum map showing the courses in which the program's educational and (if appropriate) career objectives will be taught and assessed	Section 2, Item 7
X	*For all programs*, a catalog description for each existing course that is part of the proposed graduate major program	Section 3, Item (b)
X	*For all programs with new courses,* syllabi for all new courses in a proposed graduate program	Section 3, Item (c)
X	*For programs requiring external instruction*, a completed *External Instruction Form* and documentation required on that form	Section 3, Item (d)
X	*For programs that will depend on new faculty*, position descriptions or announcements for faculty to-be-hired	Section 4, Item (b)
X	*For all programs*, original, signed External Evaluation Reports from SUNY-approved evaluators	Section 7
X	*For all programs*, a single Institutional Response to External Evaluators' Reports	Section 8
	For programs designed to enable students to complete at least 50% of the course requirements at a distance, a *Distance Education Format Proposal*	Section 10
	For programs requiring an MPA, a *Master Plan Amendment form*	Section MPA-1

External Evaluation Report

Form 2D
Version 201-08-02

The External Evaluation Report is an important component of a new academic program proposal. The external evaluator's task is to examine the program proposal and related materials, visit the campus to discuss the proposal with faculty and review related instructional resources and facilities, respond to the questions in this Report form, and submit to the institution a signed report that speaks to the quality of, and need for, the proposed program. The report should aim for completeness, accuracy and objectivity.

The institution is expected to review each External Evaluation Report it receives, prepare a single institutional response to all reports, and, as appropriate, make changes to its program proposal and plan. Each separate External Evaluation Report and the Institutional Response become part of the full program proposal that the institution submits to SUNY for approval. If an external evaluation of the proposed program is required by the New York State Education Department (SED), SUNY includes the External Evaluation Reports and Institutional Response in the full proposal that it submits to SED for registration.

Institution: University of Albany

Evaluator Name (Please print.): Nicole Lang Beebe

Evaluator Title and Institution: Associate Professor, Distinguished Professor, The University of Texas at San Antonio

Evaluator Signature: NLBeebe

Proposed Program Title: Digital Forensics

Degree: Master of Science

Date of evaluation: July 31, 2018

I. Program

1. Assess the program's **purpose, structure, and requirements** as well as formal mechanisms for program **administration and evaluation.** Address the program's academic rigor and intellectual coherence.
    a. **Purpose:** The program is multi-faceted from the standpoint that it broadens the traditional and overly narrow digital forensics definition that has been "post-mortem" and reactive in nature. The program aims to matriculate students already possessing a strong background in networking, programming, and cybersecurity, and broadening and deepening their digital forensics knowledge and experience into one of three specific areas via three formal tracks: digital forensics, cybersecurity, and cyber operations. The presumption is a digital forensics undergrad would be pursuing an advanced degree that extends their digital forensics knowledge and understanding in either the cyber operations space or the cybersecurity space. Conversely, a cybersecurity undergrad would likely be pursuing an advanced degree in digital forensics or cyber operations, to extend their knowledge and understanding into other disparate domains from their undergrad focus – specifically more digital forensics lab work or cyber operations. This enables a singular degree to simultaneously require students to matriculate into the program with sufficient requisite knowledge, while ensuring there is minimal overlap in foundational content across the undergrad

and graduate programs. This is critical in an advanced degree program seeking to pipeline students from its existing undergrad programs.

While the purpose of the program is clear and well founded, in so far as portions of the program proposal document may be used in future marketing materials, I would suggest a minor clarification of the proposal document. In the program overview, the explanation of program tracks broadens the definition and application of digital forensics to include proactive cyber hunting and offensive/defensive cyber operations. Yet, the Program Need section defines digital forensics narrowly – reactive and "post-mortem" collection and analysis. I recommend expanding the definition of digital forensics in the Program Need section.

b. **Structure**: The program structure is well thought out and postured for success, particularly respecting scope and sequence elements. Students will enter the program in a lock-step cohort fashion once per year (Fall). They will take the same required courses with reasonably limited elective options. The limit to the number of electives, as least for the cybersecurity and digital forensics tracks, is important from a program management perspective, while still leaving some avenue for students to tailor the program to their individual goals and needs. The program proposal clearly articulates knowledge, skills and abilities (KSAs) students will obtain from each track of the program. The Program Director might consider formally mapping these KSAs to specific courses, and assigning specific program curriculum committees for each of the three tracks, although this need not be done in the program proposal document. The program contains requisite support structures, respecting recruiting/marketing, admissions, advising, and job placement services.

c. **Requirements:** The program requires students to take 30 credits (15 credits Fall, 15 credits Spring) and a 6-credit internship, COOP, or thesis during the concluding summer. The program proposal document should be clarified, as it is not clear from the very beginning that this is a one-year, intensive, full-time program. Absent that knowledge of the program structure, the first reference to the 6-credit may be construed as occurring during the summer between years 1 and 2. Elsewhere in the program proposal document, it is referred to as a concluding element of the program sequence-wise. This should be clarified. Further, the student choice is differentially referenced (first as an "internship / thesis" option, then as a "COOP / internship" option), which may cause confusion.

   Regarding the Thesis option, the program might benefit from a structured approach that *requires* the thesis advisor and topic selection, supported by a literature review already conducted, to be identified during *spring semester*. While six credits is certainly sufficient for a thesis, I question whether all students can complete a quality thesis from start to finish in a single summer semester, without the topic and committee being preselected. Requiring that topic and advisor selection occur before summer might help manage student completion risk.

d. **Program Administration:** The program will be housed within the School of Business at the University of Albany. The program will be directed by Dr. Sanjay Goel, Chair, Information Systems & Digital Forensics. The program has a robust advisory board, consisting primarily of private sector personnel. The board composition is exemplary from the perspective of prospective employers and key personnel therefrom. The board would be enhanced by additional public sector personnel, particularly prospective employers of cyber operations track students, although two key people from such organizations are on the board.

e. **Program Evaluation:** The Program Director has articulated a formal three-year curriculum refresh plan to ensure the content remains current and relevant, in addition to the standard, robust university required 7-year program assessment cycle. This is commendable and highly recommended. It would be supported by the above recommendation for formal curriculum review committees for each track. This might be formalized in the program proposal document.

f. **Academic Rigor / Intellectual Coherence:** Returning to the positive observations pertaining to the scope and sequence and KSAs outlined in the program proposal, students graduating from the program will receive academically rigorous education. The course sequence, topics per track, and

KSAs per track are intellectually coherent. The following observations were made pertaining to each track:

i. DF Track
    1. The students will be exposed to appropriate tools of the trade, scientific methodology, investigative approaches, communication of findings, etc.
    2. Anti-forensics techniques and detection mechanisms may be missing from the proposed curriculum, although it may be programmed and just not evident in the course descriptions reviewed. I recommend adding it, as needed.

ii. Cyber Security Track
    1. The program might consider exposing students to more cyber hunting platforms (e.g. Sqrrl, Infocyte, Endgame, Crowdstrike's Falcon, etc.). These tend to automate the analysis and alerting function of inherently digital forensics based analytics/indicators. These tools turn traditionally reactive, post-mortem digital forensic techniques into proactive threat hunting approaches.
    2. Memory analysis might arguably be something cybersecurity track students need to know to do proactive threat hunting well. I might suggest making BFOR 607 Computer & Memory Forensics an approved elective for this track. Such skills are needed to detect modern Advanced Persistent Threat (APT) actors and activity.
    3. Along the line of detecting APT threats, similar to the digital forensics track, anti-forensics may be missing from the curriculum and should be added if not currently programmed. It need not be a separate or additional class, but should be a significant module in one or more classes in the track.
    4. Delving into course descriptions, the data analytics component of the curriculum becomes evident and will be a strength of the program, particularly in the cybersecurity track. However, the program proposal document and the KSAs outlined for the cyber security track do not sufficiently reflect this strategically advantageous benefit of the proposed program. It is this analytics component that differentiates this track within a digital forensics M.S. from other, more 'run of the mill' incident response and risk management training and education programs.

iii. Cyber Operations Track
    1. The specified KSAs for the cyber operations track are in sync with targeted employer needs. However, I fear it may be overly ambitious. It may be that they were adapted from the requisite knowledge units outlined in the NSA/DHS CAE for Cyber Operations program. I am concerned that it will be difficult to impart the breadth and depth of knowledge proposed in this track. I suggest an informal review by one or more of the following individuals: Dr. Vassil Roussev (Univ. of New Orleans), Dr. Kara Nance (Univ. of Alaska), Dr. Sujeet Shenoi (Univ. of Tulsa), Dr. Dave Dampier (UTSA), or Dr. Greg White (UTSA).

2. Comment on the **special focus** of this program, if any, as it relates to the discipline.
    a. Three tracks in the degree include cybersecurity, digital forensics, and cyber operations. Digital forensics is taught in the context of jobs in these domains. Hence, there are three foci. The three-track approach will assist greatly in recruitment and placement efforts.

3. Comment on the plans and expectations for **self-assessment and continuous improvement**.
    a. As stated previously, the program plans to follow the University's well established, robust, and successful 7-year program evaluation process, coupled with a 3-year curriculum refresh process. My only suggestion here is to formalize the 3-year review process and stakeholder/committee assignment for accountability purposes. The only evaluation mechanism I would suggest adding is post-placement employer surveys and feeding that back into the 3-year curriculum review refresh process.

4. Discuss **the relationship** of this program to other programs of the institution and collaboration with other institutions, and assess available support from related programs.
    a. The existing undergraduate digital forensics degree program and its hosting Information Security & Digital Forensics (IS &DF) Department enjoys synergistic, complementary relationships with the College of Emergency Preparedness, Homeland Security, and Cyber Security, the College of Engineering and Applied Science, and the School of Criminal Justice. IS & DF offers cybersecurity courses to majors from these colleges. Accordingly, this program will be able to leverage those relationships from a pipelining and recruitment perspective. Clear support elements from those related programs is not evident, in the sense of reciprocal curriculum or course offerings. For example, ideally students from the cyber operations track could obtain mathematical, cryptologic, etc. KSAs from courses in the computer science program. That said, in my experience, this is an ideal that is difficult to attain in reality, because the specific knowledge units offered over the course of the entire semester long course are often not sufficiently aligned with the knowledge unit needs of the disparate degree.

5. What is the evidence of **need** and **demand** for the program locally, in the State, and in the field at large? What is the extent of occupational demand for graduates? What is the evidence that demand will continue?

    a. I have no doubt that the need and demand for this degree program exists and will support the projected enrollment figures the first two years. However, the support provided in the document is dated: (1) 2009 Bureau of Labor and Statistics projections for 2016; and (2) a 2005 citation by Denning and McGettrick (2005) suggesting that decrease in students seeking STEM degrees could be mitigated by institutions providing more specialized degrees. Is there any evidence this has in fact worked?
    b. It looks like the BLS Occupational Outlook Handbook merged the "digital forensics analysts" title in with more general "forensic science technicians" title in its current edition, which may be why the proposal uses the older number. That broader category anticipates 17% growth between 2016 and 2026, which seems too low to me, given the 2015 BLS report indicates the broader cyber job demand grew 91% between 2010 and 2014, with the demand for CISSPs is outstripping supply.
    c. There is a growing demand for STEM master's degree programs from both students and employers (http://nap.edu/24946 and http://nap.edu/25038). Specialized master's degrees are desired. For example, "The Council of Graduate Schools reported on the results of a pilot study of STEM master's programs that aimed to identify factors contributing to the successful completion of the degree (CGS, 2013). Students surveyed as part of this study cited the desire to support professional aspirations by increasing knowledge and skills as the most common reason for enrolling in a master's degree program." (http://nap.edu/25038, p. 90). The same report calls for graduate STEM education where students "acquire broad technical literacy coupled with *deep specialization in an area of interest* [emphasis added]" (p. 3) – this may be somewhat taken out of context to be used here, but I think it still retains some relevance.

II. Faculty

6. **Evaluate the faculty**, individually and collectively, with regard to training, experience, research and publication, professional service, and recognition in the field.

    I cross-referenced the per track course listing, course descriptions, proposed faculty to course mapping, and faculty (tenure track, lecturer, and adjunct) resumes/CVs. I have assessed the program staffing plan as follows:

The following courses had a plan for staffing them with instructors with relevant knowledge, skills, and abilities. I also recommended alternate instructors to be included in the program plan if amenable to the Program Director.

- BFOR 604 Mobile Forensics: John Gallo (adjunct); could also be taught by Fabio Auffant (Lecturer)
- BFOR 645 Psychology & Info. Security: Kevin Williams (faculty); could also be taught by Jungwon Kuem (faculty)
- BITM 640 Info. Security Risk Analysis: Deborah Snyder (adjunct); could also be taught by Victoria Kisekka (faculty)
- BITM 642 Computer Forensics: Fabio Auffant (Lecturer)
- BITM 644 Cyber Threats and Defense: Michael Smith (adjunct); could also be taught by Victoria Kisekka (faculty)

The following courses did NOT have a plan for staffing them with instructors, but after reviewing the resumes/CVs of department faculty, including full-time/tenure track, full-time lecturers, and part-time adjuncts, I believe the department has qualified instructors who could teach the courses as follows:

- BFOR 506 Programming for Data Analytics: could be taught by Liyue Fan (faculty)
- BFOR 511 Sys Admin & Operating Systems: could be taught by Kevin Kingsley (adjunct)
- BFOR 520 Open Source Intel. & SNA: could be taught by Devipsita Bhattacharya (faculty), or Liyue Fan (faculty)
- BFOR 607 Computer & Memory Forensics: could be taught by Fabio Auffant (Lecturer)
- BFOR 610 International Cyber Conflicts: could be taught by Kevin Salhoff (adjunct)
- BFOR 613 Multimedia Forensics: could be taught by Fabio Auffant (Lecturer)
- BFOR 620 Digital Forensics Lab Management: could be taught by Fabio Auffant (Lecturer)
- BFOR 622 Cloud Security: could be taught by Suryadipta Majumdar (faculty)
- BITM 646 Math. Models for Info. Security: could be taught by Liyue Fan (faculty)

The hiring plan for two new full-time, tenure track faculty and one new adjunct faculty member constitutes the staffing plan for the following courses:

- BFOR 516 Advanced Data Analysis
- BFOR 602 eDiscovery, Cyberlaw, & Ethics
- BFOR 615 Hacking for Pen Testing

The following courses did NOT have a staffing plan and I did NOT identify suitable instructional staff for the listed reasons:

- BFOR 516 Advanced Data Analysis (wrong course description was provided)
- BFOR 650 Cyberphysical Systems Security (did not find specific expertise in resumes/CVs provided)

The following courses had a staffing plan that concerns me:

- BFOR 611 SCADA Forensics (Kevin Salhoff, Adjunct) – I did not see SCADA forensics expertise and experience in the proposed instructor's resume.
- BITM 643 Cyber Incident Analysis (John Gallo, Adjunct) – I perceive this course as being more related to intrusion/network forensics related to hacking cases, rather than traditional post-mortem analysis of non-intrusion type case. I did not see intrusion/hacking investigation forensic expertise and experience in the proposed instructor's resume.

The following courses had a staffing plan that I was not able to assess, as a current resume/CV was not available for review.

- BFOR 647 Security Implementation: Michael Smith (Adjunct)

The following errors were noted on the proposed instructional staffing plan:

- TBH2 (full-time, tenure track) is projected for BFOR 642, however, no such course number in the track schedule or course descriptions list
- TBH3 (full-time, tenure track) is proposed for BFOR 646, however, no such course number in the track schedule or course descriptions list
- Sanjay Goel (Professor) is proposed for BITM 611, however, no such course number in the track schedule or course descriptions list

7. **Assess the faculty in terms of number and qualifications** and **plans for future staffing**. Evaluate **faculty responsibilities** for the proposed program, taking into account their other institutional and programmatic commitments. Evaluate faculty **activity in generating funds** for research, training, facilities, equipment, etc. Discuss any **critical gaps and plans for addressing them**.
    a. Please see #6 above, pertaining to faculty.
    b. I did not fully evaluate faculty activity in generating funds.

8. Evaluate credentials and involvement of **adjunct faculty** and **support personnel**.
    a. Please see #6 above, pertaining to the evaluation of adjunct faculty credentials.
    b. I did not fully evaluate credentials and involvement of support personnel.

III. Students

9. Comment on the **student population the program seeks to serve**, and assess plans and projections for student recruitment and enrollment.
    a. The program plans to aggressively recruit from existing University of Albany programs that currently enjoy healthy enrollments – computer science, digital forensics, and cyber security concentration students from College of Emergency Preparedness, Homeland Security, Cyber Security degree programs.
    b. The program's plan to enroll 16 students in Year 1 and 32 students in Year 2 is reasonable, based on both market needs and the growth profile of recent, related programs. The now four-year old undergraduate degree in digital forensics has far exceeded its projected enrollments (45, 85, 115, and 125 students in years 1-4 respectively). It now has over 200 students. Presuming <10% of the current student population from this program alone pursue an advanced degree, the proposed program's enrollment projections are reasonable. Plus, the university has other internal undergrad programs from which to recruit, not to mention planned, supported external recruiting efforts. Formally surveying currently enrolled students in pipeline majors about their likelihood to enroll in the MS in Digital Forensics might be useful for projection purposes, as well as further advertising the upcoming program.
    c. The program's media and marking plan, with support from the Office of Media & Marketing, are sufficient and commendable.
    d. There exists a concern and risk regarding curricular overlap between existing undergrad programs (computer science, digital forensics, and cybersecurity) and the proposed program. However, this risk has been identified by the Program Director who has identified the following risk mitigations: (1) program prerequisite knowledge required in programming, networking, and cybersecurity assessed and verified during the admission process (primarily verified by preferred undergraduate degrees and concentrations); (2) discouraging (through formal advisement) digital forensics undergrads from taking the digital forensics track and discouraging cybersecurity concentration students from taking the cybersecurity track; (3) minimizing the number of cross-listed course and limiting them primarily to the specialty electives.

10. What are the prospects that recruitment efforts and admissions criteria will supply **a sufficient pool of highly qualified applicants and enrollees**?

a. The program anticipates maintaining or exceeding existing School of Business minimum GPA and GMAT standards, but plans to forward all reasonable applications to the program admissions faculty committee, until steady state program admission requirement expectations can be established.
b. Program expects students to have basic knowledge of programming, networking, and information security before entering the program, as evidenced by undergraduate degrees in digital forensics, computer science, or cybersecurity (concentration).
c. Program Director is considering a summer bootcamp option for students who may need refresher coursework before entering the program.
d. Program Director might consider identifying specific leveling courses to take if/as needed, ideally during the summer semester preceding the program and offering conditional admittance upon completion of the leveling courses (even if that defers their admission a year in the event the courses cannot be taken during the summer semester prior to the program starting).

11. Comment on provisions for encouraging participation of **persons from underrepresented groups**. Is there adequate attention to the needs of part-time, minority, or disadvantaged students?

a. The University of Albany is already doing a good job here, exceeding national averages for STEM and cyber that tend to be around 15-20%. Their undergraduate digital forensics program boasts a 35% URM rate, with similar statistics for the number of females in the program.
b. The University of Albany graduate school is integral to this continued success. It recognized several years ago that URM students were not matriculating into graduate degrees at a high rate (only 3-5% at the time). They diagnosed the problem and engaged in specific efforts to raise this successfully to 28%. The graduate school office is committed to employing the same techniques in this program to ensure URM students are maximally encouraged and enabled to continue their education to the graduate level through this program. The one-year, full-time nature of the program should assist in this goal also.

12. Assess the system for monitoring **students' progress and performance** and for **advising students** regarding academic and career matters.

a. Students are encouraged (but are not required) to obtain mentors.
b. The graduate office runs a "B-minus" report to alert faculty to students with declining performance. The Program Director has a very intentional approach of reaching out to declining students to ascertain the reasons and their needs.
c. The Program Director has a successful career mentoring approach at the undergraduate degree program. I might suggest formalizing this at the graduate level, to ensure it happens quickly, as the one-year nature of the program means students must get paired up with potential employers for internships and COOPs from the very beginning. However, the career fair, resume book, advisory board functions are all very supportive regarding career mentoring and placement.

13. Discuss prospects for graduates' post-completion success, whether **employment, job advancement, future study, or other outcomes related to the program's goals.**

a. The program includes three tracks: cybersecurity, digital forensics, and cyber operations – specifically training students in digital forensics for different careers where their digital forensics knowledge will be applied in different contexts, for different purposes. This is a strength, although the program might want/need to do some education of potential employers to ensure they understand the value of the degree/track approach. Many employers looking for a cyber operator or a proactive cyber hunter do not currently understand that a digital forensics education contextually set in cyber operations or cyber security gives them what they need in employees.
b. A review of the curriculum (limited to course descriptions) suggests that the graduates will be attractive to recruiters from intelligence agencies, law enforcement, private industry, consulting

firms, investigators, and employers of security analysts. The following suggestions are offered from an advisory perspective only. The current program plan need not be modified to accommodate these suggestions:

i. Add natural language processing and analytics tools to the Programming for Data Analytics, Advanced Data Analytics, and/or Open Source Intelligence and Social Network Analysis courses
ii. Modify the Advanced networking course description to reflect more advanced networking topics and differentiate it from the prerequisite networking knowledge expected of incoming students.
iii. Add knowledge and experience analyzing underlying data structures to the mobile forensics class, so that students can accomplish physical level analysis in addition to more standard tool-based data extraction and analysis based techniques.
iv. Consider expanding the scope of the SCADA forensics classes to include other industrial control system and cyber physical system communication/networking protocols, "smart" technologies and grids, and potentially even Internet of Things (IoT) protocols (although this latter item might be better placed in the Cloud Security course.
v. Consider expanding the scope of the Cloud Security course to Cloud Security and Forensics.
vi. Consider adding information security knowledge standards and indicators of compromise standards, frameworks, and languages to the Cyber Incident Analysis course.

IV. Resources

14. Comment on the adequacy of physical **resources** and **facilities**, e.g., library, computer, and laboratory facilities; practica and internship sites or other experiential learning opportunities, such as co-ops or service learning; and support services for the program, including use of resources outside the institution.

a. Program includes a 6-credit internship/COOP/thesis during the concluding summer of the program. The Program Director is actively and personally involved in student placement with significant past success and an active board to facilitate this.
b. Library resources are sufficient, with electronic subscriptions to critical publication databases and journals. Students have the library resources needed to complete course projects and the Thesis option.
c. Computing and laboratory facilities are sufficient respecting teaching space, student work space, instructional support, and software licenses. While no one I interviewed suggested that the hardware resources currently in the labs were inadequate, my experience suggests that greater computing power and better monitors at the fingertips of the students in the labs might improve student satisfaction with forensic software tools and performing lab work for extended periods of time.

15. What is the **institution's commitment** to the program as demonstrated by the operating budget, faculty salaries, the number of faculty lines relative to student numbers and workload, and discussions about administrative support with faculty and administrators?

a. I did not explore faculty salaries.
b. The number of faculty, considering both tenure track and adjunct faculty appears sufficient in light of the two new faculty lines approved for the program. However, if/as the program grows to multiple sections of the classes, additional faculty lines and/or adjuncts will be needed.
c. I noted no deficiencies in administrative support, student advising support, or budget.

V. Summary Comments and Additional Observations

16. Summarize the **major strengths and weaknesses** of the program as proposed with particular attention to feasibility of implementation and appropriateness of objectives for the degree offered.
    a. STRENGTHS:
        i. The three-track program has many benefits. It will increase recruitment and job placements by increasing the 'surface area' of the program's reputation.
        ii. The program proposal clearly identifies student learning outcomes for each track in the form of knowledge, skills, and abilities.
        iii. The Program Director understands the nature of fields/jobs this program serves changes technologically at a very rapid pace and plans to support and direct a 3-year curriculum refresh cycle. This will keep the program rigorous and relevant.
        iv. The 6-credit internship/CO-OP/Thesis option is a distinct strength, providing practical experience and increased job placement potential for students who will enter the workforce upon graduating, and providing vital research opportunities for students considering pursuing a Ph.D. program. The field is in desperate need of more college faculty in this area. Providing a Thesis option may increase such recruitment.
        v. The administrative/programmatic support of the Graduate Office and Advising is evident and important.
    b. WEAKNESSES:
        i. The program staffing plan has some gaps and inconsistencies that need to be addressed. I don't think any of these are insurmountable risks to the program, but rather things that should be cleared up as soon as possible to ensure the program is properly staff instructionally.
        ii. While the three tracks are rigorous and relevant as-is, the cybersecurity track could be improved, in my opinion, by focusing more on the technological aspects of proactive cyber threat hunting, using digital forensics techniques to detect latent intrusions and advanced persistent threats, as opposed to simply responding to those detected by tools and personnel. Students should be exposed to current threat hunting platforms and apply the programmed analytics to the detection of such threats.

17. If applicable, particularly for graduate programs, comment on the ways that this program will make a **unique contribution** to the field, and its likelihood of achieving State, regional and/or national **prominence**.
    a. I'm confident that the existing program plan and this evaluation thus far clearly communicates the unique contribution the proposed program will make and that it will indeed achieve state, regional, and national prominence.

18. Include any **further observations** important to the evaluation of this program proposal and provide any **recommendations** for the proposed program.
    a. All observations and recommendations have been stated already.

SUNY The State University of New York

External Reviewer Conflict of Interest Statement

I am providing an external review of the application submitted to the State University of New York by:

University of Albany - SUNY

The application is for:

A) New Degree PROGRAM Authority

Master of Science in Digital Forensics

(Title of Proposed Program)

I affirm that I:

1. am not a present or former employee, student, member of the governing board, owner or shareholder of, or consultant to the institution that is seeking approval for the proposed program or the entity seeking approval for new degree authority, and that I did not consult on, or help to develop, the application;

2. am not a spouse, parent, child, or sibling of any of the individuals listed above;

3. am not seeking or being sought for employment or other relationship with the institution/entity submitting the application?

4. do not have now, nor have had in the past, a relationship with the institution/entity submitting the application that might compromise my objectivity.

Name of External Reviewer (please print): Nicole L. Beebe

Signature: NLBeebe

External Evaluation Report

Form 2D

Version 201-08-02

The External Evaluation Report is an important component of a new academic program proposal. The external evaluator's task is to examine the program proposal and related materials, visit the campus to discuss the proposal with faculty and review related instructional resources and facilities, respond to the questions in this Report form, and submit to the institution a signed report that speaks to the quality of, and need for, the proposed program. The report should aim for completeness, accuracy and objectivity.

The institution is expected to review each External Evaluation Report it receives, prepare a single institutional response to all reports, and, as appropriate, make changes to its program proposal and plan. Each separate External Evaluation Report and the Institutional Response become part of the full program proposal that the institution submits to SUNY for approval. If an external evaluation of the proposed program is required by the New York State Education Department (SED), SUNY includes the External Evaluation Reports and Institutional Response in the full proposal that it submits to SED for registration.

Institution:

Evaluator Name (Please print.): John D'Arcy

Evaluator Title and Institution: Associate Professor, University of Delaware

Evaluator Signature:

Proposed Program Title: MS Digital Forensics

Degree: MS

Date of evaluation:

I. Program

1. Assess the program's **purpose, structure, and requirements** as well as formal mechanisms for program **administration and evaluation.** Address the program's academic rigor and intellectual coherence.

   The MS program being reviewed is a one-year program (fall, spring, and summer). The purpose of the program is to train students in the growing field of cyber security. The program has three tracks that are targeted towards three different audiences, i.e. forensic analysts for law enforcement agencies, security analysts for public and private sector organizations, and cyber intelligence analysts for intelligence agencies. The program starts in the fall semester in which the curriculum is mostly common across the three tracks. There are four core courses in the security and forensics track with one elective course. The second semester is different for the two tracks with four core courses and one elective course. The cyber operations track is different from the other two tracks and does not have electives. All three tracks have an internship/thesis requirement.

   Based on my review of the curriculum and discussion with the program creator/director (Sanjay Goel), I found the program to be rigorous and comprehensive. Courses in all three concentrations are well balanced and sufficient to cover the material required for the intended domains. The electives are interesting and will provide students sufficient options to choose from. I found the program innovative and all three tracks to be attractive. I was

especially impressed by the cyber operations track that will train individuals for cyber operations in intelligence agencies.

The program has a clearly defined admission criteria and an evaluation plan with the support infrastructure in place both within the School of Business and the office of Graduate Programs. Due to the rapidly changing nature of the field, I would suggest a review of the curriculum every three years and revisions as necessitated by the changes in the field.

2. Comment on the **special focus** of this program, if any, as it relates to the discipline.

The focus of the program is on cyber analytics (security, forensics, and intelligence) which is different from most other programs that I have encountered and are focused on traditional modes of security (i.e., protection of computers and networks). As information systems become more complex, the need for security analytics that can *analyze* incidents and provide in-depth visibility into computers and networks will continue to increase. All three tracks in the program focus on analytics which makes it both unique and attractive.

The program is focused on students who are looking for a short but intense program that will make them workforce ready. The rigorous program completed over one year will be very attractive to both fresh undergraduates and working professionals seeking to upgrade their knowledge base by taking some time off from work.

3. Comment on the plans and expectations for **self-assessment and continuous improvement**.

Based on my review of the documentation, there is a 7-year assessment cycle for this program in line with the other programs of the School of Business. The assessment will be done through the quality of student work in the program, student surveys, and focus groups. There will also be an annual assessment based on student curricular work and surveys.

The cyber operations track of the program will be put up for National Security Agency (NSA) accreditation which will require a review of the program every five years. Given the rapidly changing nature of the field, I would recommend a three-year curriculum review of all the concentrations to stay in tune with the evolution of the field.

4. Discuss **the relationship** of this program to other programs of the institution and collaboration with other institutions, and assess available support from related programs.

The program fits well within the School of Business. The BS in Digital Forensics has an applied focus and the employment stream is in line with the other programs of the School. The support system in the School is well positioned to support the success of the program including advisement and student support systems, as well as career services. During my visit, I met with employees who work in graduate student advisement and there was clear support (and excitement) for the program from their end. As well, in my conversations with the Dean (Hany Shawky) and Associate Dean (Suraj Commuri) there was strong management support for the program.

The College of Emergency Preparedness, Homeland Security, and Cyber Security (CEHC) is another unit of the University that is engaged in cyber security programs. Cyber security students in CEHC take several courses in the School of Business which brings synergy across the two colleges. I believe the focus of CEHC is on policy and social science compared to the more technical and management focus in the School of Business.

5. What is the evidence of **need** and **demand** for the program locally, in the State, and in the field at large? What is the extent of occupational demand for graduates? What is the evidence that demand will continue?

There is a large unfulfilled demand for cyber security and digital forensics professionals with over 300,000 openings nationwide (https://www.cyberseek.org/heatmap.html). With the growth of cyber physical systems

(smart grid, connected vehicles, and implantable medical devices) the threat landscape grows exponentially and to address this challenge, we will require well trained forensics/security analysts. The focus of the program on security analytics makes this program especially attractive to this growing market segment. The students from the program can work as security/forensics analysts in the public and private sectors, cyber intelligence analysts, cyber risk analysts, and security consultants. I see a strong growth potential for the program and it clearly addresses a need at the state and national levels.

II. Faculty

6. **Evaluate the faculty**, individually and collectively, with regard to training, experience, research and publication, professional service, and recognition in the field.

   The faculty consist of a diverse of group of traditional (full-time) academics who have taught and published in the areas of cyber security and digital forensics, as well as practitioners (adjuncts) who have extensive industry and government experience in these domains. The creator/director of the program (Sanjay Goel) is well known in the academic research realm, having produced an extensive publication record in the areas of cyber security and digital forensics (1272 citations on Google Scholar, as of 7/31/18). He also founder of a well-known conference for cyber security research and practice, the Annual Symposium on Information Assurance (ASIA), which is held annually in downtown Albany, NY. This is a high profile event that attracts academics and practitioners from around the globe. Through this event, faculty from the program have excellent opportunities to stay abreast of developments in the cyber security and digital forensics fields, and thereby apply state-of-the-art knowledge to the classroom.

   The department of Information Security and Digital Forensics has faculty which have been with the program from the start and the other faculty in the department are newly hired assistant professors who are on tenure- track. They also have a lecturer who was the head of Computer Crime Division for New York State. I have looked at each of the faculty profiles and met with some of them during my evaluation visit. As a group they have a strong background in cyber security and digital forensics and have been trained at some of the top universities in the world (e.g., Emory University, University of Arizona, University of Wisconsin-Madison). I believe they have requisite skills to make this a viable program for the long term. Fabio Auffant earned his MS degree in Digital Forensics Management from Champlain College and brings with him over 27 years of extensive technical training in the NYS Police, mainly in the Cyber Crime Unit. Dr. Devipsita Bhattacharya earned her PhD from the University of Buffalo in Management Information Systems. Dr. Liyue Fan received a PhD from Emory University in Computer Science and Informatics. Dr. Victoria Kisekka earned her PhD from the University of Buffalo in Management Science and Systems. Dr. Jungwon Kueng is a recent addition to the faculty for the program with a PhD in Operation and Information Management from the University of Wisconsin – Madison. Dr. Lee Spitzley is another addition to the team earning his PhD in Business Administration – Management Information Systems from the University of Arizona. Dr. Suryadipta Majumdar earned a PhD in Information & Systems Engineering from Concordia University. Besides the full-time academics, the program has many adjunct faculty on staff that have many years of experience throughout the government and private sector.

7. **Assess the faculty in terms of number and qualifications** and **plans for future staffing**. Evaluate **faculty responsibilities** for the proposed program, taking into account their other institutional and programmatic commitments. Evaluate faculty **activity in generating funds** for research, training, facilities, equipment, etc. Discuss any **critical gaps and plans for addressing them**.

   All the faculty are well qualified to teach in the program through their educational qualifications and work experience. Currently they have 7 tenured/tenure-track faculty with a 2+2 course load during the academic year and one lecturer with 3+3 teaching load. The department runs three other programs, a BS in Digital Forensics, an MBA concentration in Cyber Security, and a Graduate Certificate in Information Security. They have the requisite faculty mapped to the classes they will teach. Additionally, 2 faculty hires have been allocated for this program. With the existing and new hires, the department will be able to adequately staff the program.

Sanjay Goel has also received over 25 grants since starting at the University in 2001, which total over ten million dollars from federal sources (National Science Foundations, U.S. Department of Education, National Institute of Justice, and Bureau of Justice Assistance), foundations and private corporations (Blackstone Foundation, AT&T Foundation, James S. McDonnell Foundation, Palantir Corporation), and New York State (Office of Cyber Security, New York State Energy Research and Development Authority). With his work on complex self-organizing systems in transportation and smart grid, the Center for Forensics Analytics of Complex Energy and Transportation Systems (FACETS) was created at the University at Albany. Such a record of grant funding is very rare in business schools. Liyue Fan has received a CRII grant recently. Faculty are engaged in grant writing and given the culture of the department and leadership of the Chair, I am fully confident that the department will be very successful in additional obtaining grants, which should help further support the program.

There are two teaching computer laboratories with their own isolated networks where most of the teaching is done for the department. There are adequate resources to purchase software to support the labs (e.g. FTK, ENCASE. Paraben etc.) and one research lab that is a part of the FACETS Center. Currently, the University is building a special laboratory for the new MS program which will have offense and defense capabilities. The University is supporting the development of the laboratory. The Dean of the School of Business has expressed support for maintenance and upgrade of the laboratory.

8. Evaluate credentials and involvement of **adjunct faculty** and **support personnel**.

As noted above, the faculty include practitioners (adjuncts) with extensive industry and government experience. They have excellent credentials, including management experience in several Fortune 500 companies, which span multiple industries. Some also have experience in the digital forensics operations of state and federal law enforcement agencies. One is a lawyer with extensive experience in the area of cyber-crime. For the adjunct faculty that I did not meet in person, I reviewed their credentials and each is well positioned to teach in the program and contribute their practical experiences to the benefit of the students.

From my observations and conservations during my visit, the support personnel are competent and plan to be strongly engaged in the program. The Information Security and Digital Forensics Department and School of Business both have personnel in place who have worked in administering and supporting graduate programs, and their expertise in this area should help enhance the student experience. The program will also utilize the School of Business's advisement services, which have been functioning for 40 years.

III. Students

9. Comment on the **student population the program seeks to serve**, and assess plans and projections for student recruitment and enrollment.

The program seeks to serve students both from the University at Albany and other nearby colleges and universities majoring in digital forensics, cyber security, informatics and computer science. Thirty percent of students are anticipated to come from programs outside of New York State, 1/3 of which are projected to be international students. Both traditional and non-traditional students (part-time) are expected to be involved in the program. It is anticipated that 16 students will enroll in the program to start and that the program will grow to 32 students within five years. These numbers are driven by discussions with partners from industry as well as analyzing the offerings at other universities that have similar programs. Student recruitment will take place through a sustained media and marketing campaign that will be directed by a task force of representatives from the program and the University at Albany's media and marketing department. The marketing campaign will feature a rich online media presence as well as offline recruitment materials.

10. What are the prospects that recruitment efforts and admissions criteria will supply **a sufficient pool of highly qualified applicants and enrollees**?

The admissions criteria are well suited to ensure that applicants will be well qualified for the program. First, students must have achieved at a high level at the undergraduate level and must come from a computing-related field, such as cyber security, computer science, digital forensics, or information science. Their coursework must demonstrate core competencies in networking, databases, programming, cyber security and operating systems fundamentals. Additionally, they will be required to show graduate readiness by taking the GRE or GMAT exam prior to applying. Given the current undergraduate offerings at the university and across the state, as well as the international student pipelines that the program has developed, it seems likely that there is a large body of students that can meet these demands.

11. Comment on provisions for encouraging participation of **persons from underrepresented groups**. Is there adequate attention to the needs of part-time, minority, or disadvantaged students?

The program endeavors to utilize university offices and programs, such as the office of Access and Academic Enrichment to assist with the enrolling of students from underrepresented populations. The international pipelines proposed could serve as another way of expanding the reach of cyber security education to underserved populations. The role of women in the recruitment process will help the program recruit women (who are traditionally an underserved population in the STEM area). This program is primarily focused on full-time students completing their work in one year. To accommodate part-time students most classes will be offered in the evenings where working professionals can take some classes.

12. Assess the system for monitoring **students' progress and performance** and for **advising students** regarding academic and career matters.

There is a comprehensive progress and performance framework for the proposed program. The university requires a 7-year internal assessment cycle for its programs, but this program will be evaluated by external reviewers every three years. Additionally, the cyber operations track will be reviewed every five years to maintain its NSA Center of Academic Excellence in Cyber Operations certifications. Annual assessments of five key metrics will be performed based on student examinations and surveys. These metrics are student satisfaction, faculty instruction quality, assessment of learning goals, student placement, and enrollment.

Faculty mentors, as well as the well-regarded School of Business Office of Graduate Enrollment, will advise students on their choices of electives to line up with career goals.

13. Discuss prospects for graduates' post-completion success, whether **employment, job advancement, future study, or other outcomes related to the program's goals.**

The program's focus on job placement, including the Cyber Jobs Fair and Intelligence Day, will ensure that students have ready access to employers, and should see successful job placement. Opportunities to interact with faculty research mentors will provide ready access to paths for further education at the doctoral degree level. Continuing feedback from the industry advisors on the Cyber Advisory Board will ensure that the program will remain responsive to industry needs in the future. NSA and National Institute of Standards and Technology (NIST) course mappings ensure that the program's current course offerings provide the skills needed for today's workforce.

IV. Resources

14. Comment on the adequacy of physical **resources** and **facilities**, e.g., library, computer, and laboratory facilities; practica and internship sites or other experiential learning opportunities, such as co-ops or service learning; and support services for the program, including use of resources outside the institution.

Based on the documentation and conversations with the program creator/director, the university intends to add additional laboratory/classroom space to support the program. The facilities that support the undergraduate digital

forensics program are state of the art and well suited to support the demands of hands on instructions. The University libraries provide an extensive array of reference materials to support the students. The Massry Center for Business, where the program is to be housed, is a modern and comfortable building of recent vintage that has extensive space for student collaboration in additional to state of the art classroom space.

From our discussions, the creator/director has developed a concept of a virtual backpack through a grant from the National Science Foundation (NSF) that will provide students with their own virtual machine with all the necessary software pre-loaded for each semester. This will be rolled out with the program, creating a uniform computing environment for all students and streamlining the administrative process. Additionally, the concept of flipped classroom is already well integrated in the program at the undergraduate level (for several courses) and could also be used in this MS program in the future.

15. What is the **institution's commitment** to the program as demonstrated by the operating budget, faculty salaries, the number of faculty lines relative to student numbers and workload, and discussions about administrative support with faculty and administrators?

There is a commitment to hire two new faculty members for the program in the next two years. Based on my conversations with the program creator/director, that will be sufficient for the program along with the usage of existing faculty. There is an initial startup cost of purchasing equipment for the lab and then a recurring cost of $5,000 for maintenance. The license fee for software for the students will be covered by the students through their own books and supplies budgets. I would encourage the lab budget to be at least 10,000 dollars each year to ensure adequate software and maintenance. I spoke with the Dean (Hany Shawky) and Associate Dean (Suraj Commuri) of the School of Business both of whom were very supportive of the program and expressed their desire to support the program. Additionally, I spoke with the Dean of Graduate Studies (Kevin Williams) who indicated full administrative support of the program.

V. Summary Comments and Additional Observations

16. Summarize the **major strengths and weaknesses** of the program as proposed with particular attention to feasibility of implementation and appropriateness of objectives for the degree offered.

The major strengths of the program are (1) the integration analytics into all three tracks, (2) the departure of security education as consisting of theories and methods pertaining to solely the protection of computers and networks, but instead to encompass the analysis of and recovery from security incidents (which we know are now a fact of life for almost all organizations, as opposed to anomalous activities), (3) the extensive practical experience of faculty, particularly those adjuncts who have worked in the area of cyber crime, and (4) and active and engaged advisory board that is dedicated to the program and should keep its content up to date and relevant to practice.

In terms of weaknesses (and I would consider this a potential weakness as opposed to an existing weakness), I encourage those who are charged with deciding who is admitted into the program to be highly selective and transparent to the students in terms of expectations for success. This is an intense program. The fact that it can be completed in one year will likely be an attractive feature; yet, those students who are not fully committed will likely not make it through. Hence, proper vetting at the admission stage is essential.

17. If applicable, particularly for graduate programs, comment on the ways that this program will make a **unique contribution** to the field, and its likelihood of achieving State, regional and/or national **prominence**.

I would consider the aforementioned strengths of the program (in response to question #16 above) to also be ways in which the program can make a unique contribution. Particularly, the infusing of cyber security/digital forensics education with analytics is a unique aspect of the program that separates it from other programs that I

have seen. As well, the cyber operations track, which is geared toward producing graduates that can work in cyber intelligence, is a unique aspect of the program that should draw national attention. Clearly, the program is responding to critical national need in this regard.

18. Include any **further observations** important to the evaluation of this program proposal and provide any **recommendations** for the proposed program.

I believe that the program is well positioned for long term success. I also think it can be used an a tool to attract faculty to the university, and thus I encourage the university to commit additional faculty lines (possibly in the future) as the program gets off the ground and continues to grow.

SUNY The State University of New York

External Reviewer Conflict of Interest Statement

I am providing an external review of the application submitted to the State University of New York by:

(Name of Institution or Applicant)

The application is for (circle A **or** B below) A)

New Degree Authority

B) Registration of a new academic program by an existing institution of higher education:

(Title of Proposed Program)

I affirm that I:

1. am not a present or former employee, student, member of the governing board, owner or shareholder of, or consultant to the institution that is seeking approval for the proposed program or the entity seeking approval for new degree authority, and that I did not consult on, or help to develop, the application;

2. am not a spouse, parent, child, or sibling of any of the individuals listed above;

3. am not seeking or being sought for employment or other relationship with the institution/entity submitting the application?

4. do not have now, nor have had in the past, a relationship with the institution/entity submitting the application that might compromise my objectivity.

Name of External Reviewer (please print):

John D'Arcy

Signature:

RESPONSE TO REVIEWER COMMENTS

There were two independent reviewers who are experts in this field formally review the program. We have incorporated the suggestions of the reviewers and have addressed them in the revised proposal. A point by point response to all of their queries is attached to this submission letter. A point by point response is provided in response to the feedback received from Dr. Darcy (Reviewer 1) and Dr. Bebee (Reviewer 2)

REVIEWER 1 COMMENTS

Reviewer 1:
I encourage those who are charged with deciding who is admitted into the program to be highly selective and transparent to the students in terms of expectations for success. This is an intense program. The fact that it can be completed in one year will likely be an attractive feature; yet, those students who are not fully committed will likely not make it through. Hence, proper vetting at the admission stage is essential.

Response:
The GPA and standardized testing scores will be higher than those of other School of Business programs to ensure that only top-teir students are accepted into the program. This includes a 3.2 grade point average, a 580 GMAT score or a 700 on the GRE.

REVIEWER 2 COMMENTS

Comment:
I would suggest a minor clarification of the proposal document. In the program overview, the explanation of program tracks broadens the definition and application of digital forensics to include proactive cyber hunting and offensive/defensive cyber operations. Yet, the Program Need section defines digital forensics narrowly – reactive and "post-mortem" collection and analysis. I recommend expanding the definition of digital forensics in the Program Need section.
Response:
The definition portion of the Program Need section was changed to include definitions relating to each track of the program rather than just a definition of Digital Forensics.

Comment:
The program proposal document should be clarified, as it is not clear from the very beginning that this is a one-year, intensive, full-time program. Absent that knowledge of the program structure, the first reference to the 6-credit may be construed as occurring during the summer between years 1 and 2. Elsewhere in the program proposal document, it is referred to as a concluding element of the program sequence-wise. This should be clarified. Further, the student choice is differentially referenced (first as an "internship / thesis" option, then as a "COOP / internship" option), which may cause confusion.
Response:
Previously stated the length of the program to be one year. It was modified to clarify that the occurrence of the summer potion of the program will take place after all course work has been completed. Additionally, it is specified that that fifteen credits will be taken in both the fall and spring semesters.

All references to the summer work for the program now read internship/thesis option.

Comment:
Regarding the Thesis option, the program might benefit from a structured approach that requires the thesis advisor and topic selection, supported by a literature review already conducted, to be identified during spring semester. While six credits are certainly sufficient for a thesis, I question whether all students can complete a quality thesis from start to finish in a single summer semester, without the topic and committee being preselected. Requiring that topic and advisor selection occur before summer might help manage student completion risk.

Response
The program requirements section was changed to incorporate guidance that each student find an advisor, define the problem they will research and perform a literature review prior the conclusion of the spring semester. Over the summer they will only carry out their research and write their thesis. This will ensure that students are placed on a realistic timeline that will allow them to succeed in the development of a high-quality thesis.

Comment:
The board would be enhanced by additional public sector personnel, particularly prospective employers of cyber operations track students, although two key people from such organizations are on the board.

Response:
Aileen Judd, who retired from the National Security Agency in 2018, was added to the advisory board. Additionally, four members of the board are from the public sector, including its director. The board was developed to reflect the makeup of the local cybersecurity landscape, which includes public sector cyber security by nature of Albany being the states capital. Sanjay Goel is the Associate Dean for Cyber Security at the University at Albany, Deborah Snyder is the Chief Information Security Officer (CISO) for New York State Information Technology Services, Matt Anglin holds the same position for the New York State Independent Service Operator, and Marty Manjak is the CISO for the University at Albany. The board constitution is dynamic and we will surely continue to enhance our board with public sector representation as appropriate.

Comment:
The Program Director has articulated a formal three-year curriculum refresh plan to ensure the content remains current and relevant, in addition to the standard, robust university required 7-year program assessment cycle. This is commendable and highly recommended. It would be supported by the above recommendation for formal curriculum review committees for each track. This might be formalized in the program proposal document.

Response:
The following protocol was added to the proposal for the three-year assessment cycle: "In addition, to this mandatory assessment in 7-year we will conduct an informal review and assessment half-way through the University mandated assessment cycle. This will primarily be done to align our programs with the standards defined by NSA/NIST for ensuring relevance in the work place. Additionally, this will support re-accreditation with the NSA Center of Academic Excellence status for the program. The program will be mapped to national standards; post placement employer surveys will be conducted to gauge the how well our students meet the needs if their employers, and the assessment/critique of the advisory board will be solicited to update the curriculum. We will also survey graduates with respect to the relevance and use of knowledge, skills and competencies acquired in the M.S. program."

Comment:
The program might consider exposing students to more cyber hunting platforms (e.g. Sqrrl, Infocyte, Endgame, Crowdstrike's Falcon, etc.). These tend to automate the analysis and alerting function of inherently digital forensics-based analytics/indicators. These tools turn traditionally reactive, post-mortem digital forensic techniques into proactive threat hunting approaches.

Response:
A cyber threat hunting course (BFOR 632) was added to the cyber defense and cyber operations curriculum based on this recommendation.

Comment:
Anti-forensics techniques and detection mechanisms may be missing from the proposed curriculum, although it may be programmed and just not evident in the course descriptions reviewed. I recommend adding it, as needed.
Response:
While the Digital Forensics track does not include a specific ant-forensics curriculum, anti-forensics is a strong component of some of the classes in the track. In the Mobile Forensics class, anti-forensics is an implicit challenge from issues posed by smartphone encryption and remote data destruction. The Multimedia Forensics class also features a large anti-forensics component, as students are required to face the challenges posed to forensic examiners by file extension modification, encrypted containers, and steganography.

Comment:
Memory analysis might arguably be something cybersecurity track students need to know to do proactive threat hunting well. I might suggest making BFOR 607 Computer & Memory Forensics an approved elective for this track. Such skills are needed to detect modern Advanced Persistent Threat (APT) actors and activity.
Response:
Computer and Memory Forensics (BFOR 607) was incorporated as an elective for the cybersecurity track based on this recommendation.

Comment:
Along the line of detecting APT threats, similar to the digital forensics track, anti-forensics may be missing from the curriculum and should be added if not currently programmed. It need not be a separate or additional class but should be a significant module in one or more classes in the track.
Response:
The newly created Cyber Threat Hunting Class, BFOR 632 will incorporate anti-forensics techniques, as these will be critical to understanding the how threats can be hidden from security tools.

Comment:
Delving into course descriptions, the data analytics component of the curriculum becomes evident and will be a strength of the program, particularly in the cybersecurity track. However, the program proposal document and the KSAs outlined for the cyber security track do not sufficiently reflect this strategically advantageous benefit of the proposed program. It is this analytics component that differentiates this track within a digital forensics M.S. from other, more 'run of the mill' incident response and risk management training and education programs.
Response:
The KSAs were changed to reflect this, incorporating the machine learning and natural language processing

Comment:
The specified KSAs for the cyber operations track are in sync with targeted employer needs. However, I fear it may be overly ambitious. It may be that they were adapted from the requisite knowledge units outlined in the NSA/DHS CAE for Cyber Operations program. I am concerned that it will be difficult to impart the breadth and depth of knowledge proposed in this track. I suggest an informal review by one or more of the following individuals: Dr. Vassil Roussev (Univ. of New Orleans), Dr. Kara Nance (Univ. of Alaska), Dr. Sujeet Shenoi (Univ of Tulsa), Dr. Dave Dampier (UTSA), or Dr. Greg White (UTSA).
Response:

The KSAs listed were adapted from the from the National Security Agency's Center of Academic Excellence in Cyber Operations program as the reviewer suspected. While the KSAs listed by the NSA are specific checkmarks that used for program accreditation, for the purposes of a program proposal they are too in depth. The developers of the program reformulated these highly granular KSAs into higher level KSAs that can better provide strategic direction for the program.

Comment:
My only suggestion here is to formalize the 3-year review process and stakeholder/committee assignment for accountability purposes. The only evaluation mechanism I would suggest adding is post-placement employer surveys and feeding that back into the 3-year curriculum review refresh process.
Response:
As stated above, the review process was formalized as follows: "In addition, to this mandatory assessment in 7-year we will conduct an informal review and assessment half-way through the University mandated assessment cycle. This will primarily be done to align our programs with the standards defined by NSA/NIST for ensuring relevance in the work place. Additionally, this will support re-accreditation with the NSA Center of Academic Excellence status for the program. The program will be mapped to national standards; post placement employer surveys will be conducted to gauge the how well our students meet the needs if their employers, and the assessment/critique of the advisory board will be solicited to update the curriculum. We will also survey graduates with respect to the relevance and use of knowledge, skills and competencies acquired in the M.S. program."

Comment:
I have no doubt that the need and demand for this degree program exists and will support the projected enrollment figures the first two years. However, the support provided in the document is dated: (1) 2009 Bureau of Labor and Statistics projections for 2016; and (2) a 2005 citation by Denning and McGettrick (2005) suggesting that decrease in students seeking STEM degrees could be mitigated by institutions providing more specialized degrees. Is there any evidence this has in fact worked?
Response:
This was the finding from previous literature when the proposal was created. No recent articles articulating this were identified.

Comment:
It looks like the BLS Occupational Outlook Handbook merged the "digital forensics analysts" title in with more general "forensic science technicians" title in its current edition, which may be why the proposal uses the older number. That broader category anticipates 17% growth between 2016 and 2026, which seems too low to me, given the 2015 BLS report indicates the broader cyber job demand grew 91% between 2010 and 2014, with the demand for CISSPs is outstripping supply.
Response:
Cited the suggested statistics from the following sources:

i. https://www.computerworld.com/article/2495985/it-careers/demand-for-it-security-experts-outstrips-supply.html
ii. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Note:
The observations of the reviewer on the content of the courses are based on the course descriptions. As we develop detailed syllabi for the classes, we plan to incorporate all of these elements into our classes. However, we have provided point by point responses to the reviewers' suggestions.

Comment:

Add natural language processing and analytics tools to the Programming for Data Analytics, Advanced Data Analytics, and/or Open Source Intelligence and Social Network Analysis courses

Response:

Natural Language Processing (NLP) was added to the advanced data analytics class and use of NLP for intelligence gathering was added to the Open Source Intelligence class.

Comment:

Modify the Advanced networking course description to reflect more advanced networking topics and differentiate it from the prerequisite networking knowledge expected of incoming students.

Response:

Advanced Networking Course will incorporate advanced topics such as network segregation, Internet inter-domain routing, Internet security, Internet traffic measurement and analysis

Comment:

Add knowledge and experience analyzing underlying data structures to the mobile forensics class, so that students can accomplish physical level analysis in addition to more standard tool-based data extraction and analysis-based techniques.

Response:

Students will have hands-on practice in forensics labs for extracting data from phones. This experience is already programmed into the undergraduate digital forensics curriculum and can be easily scaled for the graduate level mobile forensics course.

Comment:

Consider expanding the scope of the SCADA forensics classes to include other industrial control system and cyber physical system communication/networking protocols, "smart" technologies and grids, and potentially even Internet of Things (IoT) protocols (although this latter item might be better placed in the Cloud Security course.

Response:

We are working with NYISO to include power grid elements into the SCADA forensics class.

Comment:

Consider expanding the scope of the Cloud Security course to Cloud Security and Forensics.

Response:

As the implications of the cloud on post incident forensic examinations is important to understand for security analysts, we have accepted this suggestion and have renamed the class to reflect this additional scope. The Cloud Security and Forensics course will be an elective for both the digital forensics and cyber defense tracks.

Comment:

Consider adding information security knowledge standards and indicators of compromise standards, frameworks, and languages to the Cyber Incident Analysis course.

Response:

This will be done as the curriculum for this class is modified to reflect the goals for the master's program.

Comment:

The following courses did NOT have a staffing plan and I did NOT identify suitable instructional staff for the listed reasons:

1. BFOR 516 Advanced Data Analysis (wrong course description was provided)

Response:

Liyue Fan will teach this class, who is the current instructor for BFOR 506, Programming for Data Analytics. Dr. Fan has published extensively in the field of privacy preserving data analytics,

spatiotemporal data analytics, and has teaching experience in this field, having been an instructor for Machine Learning for Data Informatics and Programming in Python prior to joining the faculty at the University at Albany.

2. BFOR 650 Cyberphysical Systems Security (did not find specific expertise in resumes/CVs provided)

Response:

This course will be taught by a new hire from, a tenure track faculty member. The instructor will have a degree in computer science, information science or similar, with a research focus on privacy preserving techniques for Cyberphysical systems or embedded device security and forensics, or a similar research focus.

Comment:

The following courses had a staffing plan that concerns me:

1. BFOR 611 SCADA Forensics (Kevin Salhoff, Adjunct) – I did not see SCADA forensics expertise and experience in the proposed instructor's resume.

Response:

While it is not clear from his resume, Kevin Salhoff has field experience performing this type of work. He has been working with the Computer Crime Laboratory for over 10 years and has practical experience in examining SCADA Systems. The tenure track faculty member who is the instructor for BFOR 650, will also be able to teach this class, as it requires a similar expertise.

2. BITM 643 Cyber Incident Analysis (John Gallo, Adjunct) – I perceive this course as being more related to intrusion/network forensics related to hacking cases, rather than traditional post-mortem analysis of non-intrusion type case. I did not see intrusion/hacking investigation forensic expertise and experience in the proposed instructor's resume.

Response:

This class will be taught by Marty Manjak, rather than John Gallo. Marty is the Chief Information Security Officer for the University at Albany and has a great deal of experience in networking and incident response. He has also served as an adjunct professor for this class before, and therefore is well suited for teaching this class. His work experience and prior teaching will allow this class to have a skilled instructor or with a network forensics focus.