UNIVERSITY SENATE

UNIVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK

Introduced by: Graduate Academic Council
                   University Planning & Policy Council

Date: April 6, 2015

PROPOSAL TO ESTABLISH A GRADUATE CERTIFICATE PROGRAM IN EMERGENCY PREPAREDNESS, HOMELAND SECURITY, AND CYBER SECURITY

IT IS HEREBY PROPOSED THAT THE FOLLOWING BE ADOPTED:

1.   That the University Senate approves the attached proposal as approved by the Graduate Academic Council and University Planning & Policy Council.

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

This form should be used to seek SUNY's approval and the State Education Department's (SED) registration of a proposed new academic program leading to a certificate (undergraduate) or an advanced certificate (graduate). 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 3 and Section 10 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] Guidance on academic program planning is available at http://www.suny.edu/provost/academic_affairs/app/main.cfm.

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.

Section 1. General Information	
Item	**Response** *(type in the requested information)*

---

[1]Use a different form if the proposed new program will lead to a degree; 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.

a) Institutional Information	Date of Proposal:	February 26, 2015
	Institution's 6-digit SED Code:	210500
	Institution's Name:	University at Albany
	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): University at 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 [✓] if not applicable**:	
c) Proposed Program Information	Program Title:	Emergency Preparedness, Homeland Security, and Cybersecurity
	Award(s) (e.g., Certificate):	Graduate Certificate
	Number of Required Credits:	Minimum [16] If tracks or options, largest minimum [ ]
	Proposed HEGIS Code:	2102 Public Administration
	Proposed 6-digit CIP 2010 Code:	44.0401 Public Administration
	If the program will be accredited, list the accrediting agency and expected date of accreditation: n/a	
	If applicable, list the SED professional licensure title(s)[3] to which the program leads: n/a	
d) Contact Person for This Proposal	Name and title: R. Karl Rethemeyer, Interim Dean, Rockefeller College	
	Telephone:518-442-5283 E-mail:kretheme@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, University at Albany	
	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 and title of partner institution's CEO:	
	Signature of partner institution's CEO (or **append** a signed letter indicating approval of this proposal):	

Version 2013-10-17

---

[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.

2.1. Program Format

Check all SED-defined <u>format, mode and other program features</u> that apply to the **entire program**.

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

b) **Modes**: [X]Standard [ ]Independent Study [ ]External [ ]Accelerated [X]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 <u>Distance Education Format Proposal</u>.*

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

2.2. Related Degree Programs

All coursework required for completion of the certificate or advanced certificate program must be applicable to a currently registered degree program at the institution (with the possible exception of post-doctoral certificates in health-related fields). Indicate the registered degree program(s) by title, award and five-digit SED Inventory of Registered Programs (IRP) code to which the credits will apply:
Title: Public Administration
Award: MPA
IRP Code: 03038

2.3 Program Description, Purposes and Planning

Introduction

On September 11, 2001, in a series of coordinated terrorist attacks, hijackers created crisis and tragedy as they crashed planes into the World Trade Center, the Pentagon, and the countryside of Pennsylvania killing more than 3,000 people in what was to become the deadliest terrorist attack on American soil. In August of 2005, Hurricane Katrina made landfall along the Gulf Coast of Louisiana, Alabama, Texas, Florida, and Mississippi. Katrina resulted in over 1,800 deaths. American industry, infrastructure and private citizens are increasingly under attack via ubiquitous computers and networks, resulting in billions of dollars in losses and threats to the US economy and even national security. There are also other hazards that have less obvious – but still important and tragic – consequences. These tragedies, and events like them, are examples of some of the most troubling risks that face modern societies. The US is hardly alone in facing them. Terrorist attacks have been catastrophic in Oslo, Mumbai, Bali, London, Istanbul and Madrid. Natural disasters like tsunamis have caused massive destruction in Indonesia, Thailand, and even precipitated a secondary nuclear disaster in Fukushima, Japan. Cyber intrusions are an endemic problem in every society where the Internet has had major penetration, and cyber attacks on critical infrastructure have reportedly caused power outages in Brazil and damaged the Iranian nuclear program. Increasingly the environment that governments and companies function in is shaped by these catastrophic risks, and the need to manage the impacts and outcomes of such events is paramount.

Increasingly, there is a blurring of corporate enterprise risk management and public sector risk management efforts. For example, the Obama Administration recently released a National Strategy for Global Supply Chain Security, a recognition that public-private distinctions and even local-national-global distinctions are more complex in this age of risk. Similarly, the Administration's recently released proposal for cyber security legislation takes seriously the need to work across government and corporate "silos."

This graduate certificate program is designed to prepare students with undergraduate degrees or previously completed master's degrees that did not train them directly or extensively for service in the fields of emergency preparedness, homeland security, and cybersecurity to be more competitive when seeking jobs in government, non-profits, and for-profits organizations.

The proposed certificate program builds on our existing concentration in homeland security in the Rockefeller College's Master of Public Administration (MPA) program and the existing homeland security option in our Public Sector Management (PSM) graduate certificate program. The newly proposed certificate will expand upon the existing offerings to include emergency preparedness and cybersecurity as explicit options, and will recognize that study and training in these domains is larger than "public management" and therefore this certificate should stand apart from the PSM certificate. Creating a stand-alone certificate will make marketing to both students and potential employers of these offerings easier and clearer and will bring our offerings into line with the institutional structure most common among our peers and competitors.

Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity
The Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity (EHC) curriculum, designed by University faculty in consultation with law enforcement, intelligence, emergency services, and public management experts, provides graduates with the foundation to become more effective homeland security and cybersecurity professionals and managers.

Students in the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity will increase their understandings of:

- The origin, nature, and impact of terrorism and cyber threats;
- Forces affecting flows of information and intelligence;
- The role of domestic criminal justice, intelligence agencies, private-sector infrastructure owners, and authorities with responsibility for responding to cyber attacks;
- Analytic, methodological, and technical skills for analyzing homeland security and cybersecurity issues;
- The institutional frameworks within which homeland security and cybersecurity exist

Requirements for the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity

The Certificate consists of five graduate-level courses. Students may concentrate in one of three tracks: Emergency Preparedness, Homeland Security, or Cybersecurity.

The following course is required of all students in the EHC certificate program, regardless of track:

- PAD 557 - Intelligence Analysis for Homeland Security

Requirements for the Emergency Preparedness Track:

The following course is required of all students concentrating in the Emergency Preparedness track:

- PAD 555 (POS 555) – Disaster, Crisis, and Emergency Management and Policy

Students may then select three additional courses from the following list with the consent of their advisor:

- PAD 504 – Data Models, and Decisions I
- PAD 505 (POS 505) – Data, Models, and Decisions II
- PAD 517 (POS 517) – Empirical Data Analysis
- PAD 518 (POS 518) – Regression Analysis
- PAD 546 – Homeland Security Risk Analysis and Risk Management
- PAD 550 – Foundations of Government Information Strategy and Management
- PAD 551 (CRJ 648) – Terrorism, Public Security and Law Enforcement
- PAD 553 – Topics in Homeland Security and Terrorism
- PAD 559 – Homeland Security: Building Preparedness Capabilities
- PAD 585 (POS 585, INF 585) – Information Technology and Homeland Security
- PAD 610 – Organizational Theory and Behavior
- PAD 624 – Simulating Dynamic Systems
- PAD 636 – Cultural Analysis of Organizations
- PAD 637 – Social and Organizational Networks in Public Policy, Management, and Service Delivery: Theory, Methods and Analysis
- PAD 705 – Research Methods II
- POS 582 – Global Security
- CRJ 504 – Applied Statistics I

4

- IST 532 – Terrorism, Public Security and Information Analysis

Requirements for the Homeland Security track:

The following course is required of all students concentrating in the Homeland Security track:

- PAD 554 (POS 554) – Political Violence, Insurgency, and Terrorism

Students may then select three additional courses from the following list with the consent of their advisor:

- PAD 504 – Data Models, and Decisions I
- PAD 505 (POS 505) – Data, Models, and Decisions II
- PAD 517 (POS 517) – Empirical Data Analysis
- PAD 518 (POS 518) – Regression Analysis
- PAD 546 – Homeland Security Risk Analysis and Risk Management
- PAD 550 – Foundations of Government Information Strategy and Management
- PAD 551 (CRJ 648) – Terrorism, Public Security and Law Enforcement
- PAD 553 – Topics in Homeland Security and Terrorism
- PAD 555 (POS 555) – Disaster, Crisis, Emergency Management and Policy
- PAD 556 – Homeland Security Intelligence
- PAD 558 – Intelligence & US National Security Policymaking
- PAD 559 – Homeland Security: Building Preparedness Capabilities
- PAD 583 (POS 583) – Global Governance
- PAD 585 (POS 585, INF 585) – Information Technology and Homeland Security
- PAD 610 – Organizational Theory and Behavior
- PAD 624 – Simulating Dynamic Systems
- PAD 625 (POS 626) Bargaining and Negotiation
- PAD 636 – Cultural Analysis of Organizations
- PAD 637 – Social and Organizational Networks in Public Policy, Management, and Service Delivery: Theory, Methods and Analysis
- PAD 705 – Research Methods II
- POS 550 – Field Seminar in Comparative Political Systems
- POS 566 – Ethnic Conflict
- POS 567 - Contentious Politics: Theory and Research
- POS 570 – Field Seminar in International Political Systems
- POS 582 – Global Security
- CRJ 504 – Applied Statistics I
- IST 532 – Terrorism, Public Security and Information Analysis

Requirements for the Cybersecurity Track:

The following course is required of all students concentrating in the Cybersecurity track:

- PAD 545 – Principles and Practices of Cybersecurity

Students may then select three additional courses from the following list with the consent of their advisor:

- PAD 504 – Data Models, and Decisions I
- PAD 505 (POS 505) – Data, Models, and Decisions II
- PAD 517 (POS 517) – Empirical Data Analysis
- PAD 518 (POS 518) – Regression Analysis
- PAD 546 – Homeland Security Risk Analysis and Risk Management
- PAD 550 – Foundations of Government Information Strategy and Management
- PAD 553 – Topics in Homeland Security and Terrorism

- PAD 558 – Intelligence & US National Security Policymaking
- PAD 583 (POS 583) – Global Governance
- PAD 585 (POS 585, INF 585) – Information Technology and Homeland Security
- PAD 624 – Simulating Dynamic Systems
- PAD 636 – Cultural Analysis of Organizations
- PAD 637 – Social and Organizational Networks in Public Policy, Management, and Service Delivery: Theory, Methods and Analysis
- PAD 705 – Research Methods II
- POS 582 – Global Security
- CRJ 504 – Applied Statistics I
- IST 532 – Terrorism, Public Security and Information Analysis
- ITM 604 – Data Communications, Computer Networking and Computer Security or ITM 644 – Introduction to Information & Cyber Security
- ITM 640 – Information Security Risk Assessment
- ITM 641 – Security Policies
- ITM 642 – Computer Forensics
- ITM 643 – Incident Handling
- ITM 645 – Psychology & Information Security
- ITM 646 – Mathematical Models for Information Security
- ITM 647 – Security Implementation
- ITM 691 – Field Study in Information Technology Management
- CSI 416/516 – Computer Communication Networks
- CSI 424/524 – Information Security
- CSI 426/526 – Cryptography
- CSI 628 – Cryptographic Protocols
- FOR 610 – International Cyber Conflicts
- FOR 611 – Supervisory Control And Data Acquisition (SCADA) Forensics
- FOR 613 – Multimedia Forensics
- INF 503 – Advanced Networking and Security
- INF 504 – Advanced Systems and Security
- INF 552 – Computer and Network Security
- INF 553 – Information Security and Privacy
- INF 554 – Human Aspects of Cyber-security
- INF 555 – Prevention and Protection Strategies in Cyber-security

---

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 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."*

Upon completion of this program, students in the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity will have an understanding of:

General
- Forces affecting flows of information, intelligence, and situational awareness (PAD 557);
- Analytic, methodological, and technical skills for analyzing homeland security and cybersecurity issues (PAD 557);

Emergency Preparedness
- The policy frameworks that govern emergency response in the US (PAD 555/POS 555)
- The institutional frameworks within which emergency response in the US operates (PAD 555/POS 555)

Homeland Security
- The origin, nature, and impact of terrorism (PAD 554/POS 554);
- The frameworks for understanding counterterrorism and counterinsurgency (PAD 554/POS 554)

Cybersecurity
- The role of domestic criminal justice, intelligence agencies, private-sector infrastructure owners, and authorities with responsibility for responding to cyber attacks (PAD 545);
- The institutional frameworks within which homeland security and cybersecurity exist (PAD 545)

---

c) 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?

This proposal intends to invest in the development of a graduate certificate program in support of initiatives contained in UAlbany's strategic investment plan, *UAlbany Impact*, that was written in response to Governor Andrew Cuomo and SUN Chancellor Nancy Zimpher's NYSUNY Challenge Grant Initiative. The proposed program intends to realize, in part, the UAlbany funded NYSUNY 2020 proposal to offer a certificate in homeland and cybersecurity that is available as both as an online program and a "standard" instructional program. The EHC graduate certificate program directly supports UAlbany's strategic initiative #4 - Public Service and Policy: Improving the Human Condition through Research on Policy and Practice. Specifically, according to *UAlbany Impact* (pg. 13):

> *UAlbany is positioned to expand its public service and policy programs to address research and workforce training and development requirements in many critical areas. There are urgent needs as government and public services are being reshaped and reformed in response to changes in the national and local economies, increased global competition for development, demographic shifts in New York State's population, and rapidly changing technologies. Homeland and international security, efforts to improve the criminal justice system and crime prevention, initiatives to address disparities in the delivery of social services and health care, and interventions to lower barriers to economic success and reduce violence and addiction are all examples of areas in which there are imoirtant issues that require study and concentrated attention.*

The proposed program in EHC will increase opportunities for students at the local, national and international levels through interdisciplinary training to strengthen their experience and training in the growing and critically important fields of emergency parparedness, homeland security, and cybersecurity and highlight the University at Albany as a center of excellence in these fields.

The proposed certificate program will concentrate on different aspects of emergency preparedness, homeland security, and cybersecurity and draw on the expertise of University faculty as well as practitioners from a wide variety of backgrounds. The program will not overlap with or negatively impact any certificate programs offered at the University at Albany, including at the College of Computing and Information or the School of Business, but rather will build upon strengths of already established programs (i.e. Rockefeller's existing concentration in homeland security in the MPA program and the existing homeland security option in the College's Public Sector Management graduate certificate program).

In terms of diversity and/or international perspectives, we expect the EHC program to attract students and potential faculty from a wide variety of backgrounds. Through Rockefeller's already established global network and by supporting various international projects, the EHC program will create additional research opportunities for motivated students and allow them to gain practical experience while emphasizing the connectedness and importance of emergency preparedness, homeland security, and cybersecurity at many levels – nationally and internationally.

---

d) How were faculty involved in the program's design?

The Rockefeller College established its original Certificate in Public Sector Management with a concentration in Homeland Security in 2004-2005 through a collaborative process involving faculty members from the Department of Public Administration and Policy, the School of Criminal Justice, and the Department of Political Science in addition to professionals from the New York State Office of Homeland Security (now the New York State Division of Homeland Security and Emergency Services – DHSES). The Department of Public Administration and Policy approved the creation of a concentration in homeland security in the MPA program in 2007. The Certificate proposed here was originally developed through a faculty committee in 2012-2013 in order to compete for NYSUNY 2020 funds. The committee's

NYSUNY 2020 proposal was then presented to the entire faculty of the Rockefeller College and was approved. When funding was awarded, the same faculty committee again collaborated to develop this document. The faculty of the Department of Public Administration and Policy was presented this document on August 14, 2014 and approved its contents unanimously.

---

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 <u>Commissioner's Regulations for the profession</u>, **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 <u>specialized form</u> for the profession to which the proposed program leads, **append** a completed form at the end of this document.

As noted above, the certificate proposed herein is a logical extension of the consultative process that began with New York State Office of Homeland Security and continues with the New York State Division of Homeland Security and Emergency Services (DHSES). The original certificate was specifically designed to meet the State's anticipated educational needs. DHSES continues to provide input into state training needs through a number of contacts, including through a joint Rockefeller College/DHSES homeland security training grant obtained in 2011 (the T-STeP program – grant DHS-11-ST-104-001) and the National Center on Security Preparedness (NCSP), a unit of Rockefeller College, which works closely with DHSES to provide training and educational services. The Director of NCSP is a public service professor at Rockefeller College who works closely on a daily basis with DHSES. He participated in the committee that developed this document.

---

f) Enter anticipated enrollments for Years 1 through 5 in the table below. How were they determined, and what assumptions were used? What contingencies exist if anticipated enrollments are not achieved?

Year	Anticipated Headcount Enrollment			Estimated FTE
	Full-time	**Part-time**	**Total**	
1	1	3	4	2.5
2	1	6	7	4
3	1	9	10	5.5
4	1	11	12	6.5
5	1	13	14	7.5

The anticipated enrollment numbers are based on (1) our existing experience with the homeland security option in the Certificate in Public Sector Management and the MPA concentration in homeland security, (2) research into existing programs at institutions around the country and in New York State, and (3) research on patterns of demand evident among students in high school. We specifically note the large number of PSAT takers in 2010 that reported security/protective services as an academic interest (4.9%), the existing unmet demand for homeland security in the New York's Capital Region as evidenced by the large number of students in community colleges with an interest in homeland security and criminal justice, and the rapid growth of the MPA concentration in homeland security, which between 2008 and 2013 grew to be the single largest concentration in the program. Additionally, our outreach to military bases indicated that there is unmet demand for graduate education among returning military members. The current offerings are not meeting that demand because (1) the existing program is not available online and (2) does not adequately address interest in cybersecurity.

For purposes of the chart above, it was assumed that a fulltime student would be enrolled in 12 credit hours and each part-time student would be enrolled in six credit hours, per semester. In reality, part-time students will be enrolled for either four or eight credit hours per semester.

Based on the current demand from students for EHC courses, we are confident that these enrollment numbers will be met, and most likely exceeded. In the rare circumstance that enrollments are not achieved, Rockefeller College will place greater emphasis on the program in its marketing and recruitment activities. If enrollments fall drastically short despite our increased efforts, the certificate could be eliminated at little or no cost as all the required and electives courses are already regularly being taught as part of other existing programs.

8

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

The certificate does not require prerequisites. Students will choose one of three tracks: Emergency Preparedness, Homeland Security, or Cybersecurity. The following course is required of all students in the EHC certificate program:

- PAD 557 - Intelligence Analysis for Homeland Security

Each track has a specific required course:

- Emergency Preparedness: PAD 555 (POS 555) – Disaster, Crisis, and Emergency Management and Policy
- Homeland Security: PAD 554 (POS 554) – Political Violence, Insurgency, and Terrorism
- Cybersecurity: PAD 545 – Principles and Practices of Cybersecurity

In addition, students must take three electives in their respective track (as noted above).

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?

Workforce Requirements. When the public thinks about homeland security, they usually focus on the eponymous federal agency – the Department of Homeland Security (DHS) – and to a lesser extent the state "siblings" that were created after the September 11th attacks. And well they should: federal DHS employs around 200,000[4] people as well as at least 200,000 private contractors.[5] This includes many previous government employees from DHS's constituent agencies (Customs and Border Patrol, the Federal Emergency Management Agency, etc.), but also many new employees in areas like intelligence analysis, critical infrastructure protection, risk management, cybersecurity, and others. However, DHS is hardly the only federal agency where such areas have grown rapidly – the Intelligence Community, the Military, and other federal agencies have also hired massively in these areas.

The overall size and scope of the US national security and homeland security bureaucracies are huge. Using the possession of a security clearance – the prerequisite for most federal homeland security and intelligence work – as a metric of total workforce in this area, a 2010 report from the General Accountability Office (GAO) suggests more than 2 million people work in this area of federal responsibility, though many are private contractors.[6] Since 2001, CNN reports that the United States has spent "hundreds of billions of dollars" on homeland security.[7]

Concurrently, there has also been a huge growth in state and local government hiring in emergency preparedness, homeland security, cybersecurity, and related fields. While some of the state and local hiring has been due to federal grant funding, which is in decline, many of these functions are being maintained despite the changing fiscal environment because these functions cannot be ignored or abandoned. Simply put, the public sector security structure is (1) quite large, (2) will require new generations of workers as those public servants brought into DHS-like structures from precursor agencies retire, and (3) continues to evolve to meet new threats.

What is generally less well understood is that the next round of growth in emergency preparedness, homeland security, and cybersecurity employment will likely happen in the private sector. While public sector employment growth in homeland security may be leveling off, there are rapidly expanding opportunities in the private sector in areas such as enterprise continuity of operations, critical infrastructure protection, and especially cybersecurity. In the private sector the number of security personnel has grown dramatically nationwide to upwards of 1.5 million people as of 2008.[8] This includes only those involved in traditional "police" or "law enforcement" functions – investigations, physical security, and loss prevention activities – but *none* of the people involved in broader risk management activities. In fact, this force of 1.5 million security personnel is nearly twice the number of sworn police officers in the United States,[9] a ratio that is likely to grow given the broader move toward privatizing functions formerly provided by government. The same trend, according

to the United Nations, is true internationally.[10] Perhaps equally important to those employed in "traditional" security roles in the private sector is the growing importance of risk management in the private sector. Emerging and expanding fields in the corporate and nonprofit sectors include areas like "Competitive Intelligence,"[11] "Enterprise Risk Management,"[12] "Continuity of Operations,"[13] and "Strategic Risk Management."[14] All of these approaches take a risk-based approach to existing private sector industries and projects.

Additionally, there is very strong evidence that corporate leaders are increasingly taking a risk management approach to dealing with threats like terrorism[15], cyber security[16], pandemic influenza[17], and other threats to their operations.[18] To effectively take this approach, these corporations will require a trained workforce.

Finally, both the public and private sectors are undersupplied in the area of cybersecurity. Informal communications with alumni working in cybersecurity suggest that there are currently at least 10,000 jobs unfilled in Washington, DC alone for lack of properly trained workers.[19] The Center for Strategic & International Studies issued a report in 2010, *A Human Capital Crisis in Cybersecurity*, that estimated "near term" demand at 10,000 to 30,000 in Federal and critical cyber infrastructure alone, with much greater demand generally because cybersecurity is embedded throughout our economy and society.[20] The US Bureau of Labor Statistics (BLS) anticipates an overall 3.9% annual growth in career opportunities in "Computer Systems Design and Related Services." This is in their top 20 areas of growth.[21] As cybersecurity is an acknowledged area of growth within this larger segment, it is reasonable to assume even higher rates of employment formation. Similarly, BLS expects high growth (22% over the period) in "Computer and Mathematical Occupations," with a median salary of $73,720 in this segment.[22] High salaries are often correlated with high student interest in a field. Areas of high demand, such as cybersecurity, command commensurately higher salaries within the field.

The relevant career areas assigned to graduates at the technical end of the cybersecurity spectrum (*i.e.* computer scientists; network, system and database administrators; computer systems analysts; computer and information system managers) are all expected to grow: "Employment growth is expected to be much faster than the average,[23] and job prospects should be excellent."[24]

In New York State, our existing partnership with DHSES and communications with the Center for Internet Security (CIS), nonprofit based in East Greenbush, NY that serves as a key resource for state, local, tribal, and territorial governments with respect to cybersecurity concerns, suggests that additional capacity is required. For instance, CIS has previously described its difficulty in finding and hiring cybersecurity analysts. Rockefeller College's existing MPA program has a 100% placement rate for completing concentrators, and we currently have more internship announcements than students to fill those internships. Additionally, we would point to several indicators of growing and/or unmet need:

- Governor Cuomo has convened several conferences on resilience and the need to improve emergency preparedness in the wake Superstorm Sandy.
- Reviews conducted by the College's National Center for Security Preparedness (NCSP) suggested that response to Sandy was hampered by "staffing, technology, and doctrine" (see pages 4 and 11 of http://projectdisaster.com/media/205727357-Sandy-Draft-After-Action-Report.pdf), particularly the lack of "trained staff" (page 11).
- New York State is adding cybersecurity requirements to bank examination processes (see http://www.forbes.com/sites/gregorymcneal/2014/05/26/banks-challenged-by-cybersecurity-threats-state-regulators-acting/).
- Governor Cuomo established the Cyber Advisory Board to address growing cyber threats in NYS (see http://www.governor.ny.gov/press/100102013-cybersecurity-advisory-board).
- New York State has continued to hire emergency preparedness personnel despite a state-wide hiring freeze (communications from DHSES personnel).

With respect to current programs: First, many community colleges offer criminal justice and first responder programs. However, there are very few educational options for professionals that operate at a managerial or event management level. Second, the primary public university option in New York State for homeland security/emergency preparedness training for managerial personnel is John Jay College in the CUNY system. There are no Upstate options in the SUNY system. Third, Upstate options that do exist for some forms of training in this domain reside at private universities that are much more expensive. For instance, Utica College offers a program in digital forensics – what could be considered "digital first response." However, the program is also not aimed at managers and is substantially more expensive then the option we propose herein.

Thus the fields of emergency preparedness, homeland security, and cybersecurity are growing quickly, changing dynamically, and creating jobs as many other fields appear to be shrinking. The growth in spending and workforce in the Department of Homeland Security represents the largest reshaping of the federal government since World War II. Yet this change may be dwarfed by the private investment in security and enterprise continuity that is still ramping up. So far, this change in prioritization and expenditure has simply not been reflected in public policy and criminal justice programs nationwide.

4 http://www.napawash.org/pc_management_studies/dhs.html
5 http://www.govexec.com/dailyfed/0210/022410e1.htm
6 http://www.fas.org/sgp/gao/gao-09-488.pdf
7 http://money.cnn.com/2011/05/02/news/economy/security_spending/index.htm
8 North American Industry Classification System (NAICS) codes 5616-56162 at
http://www2.census.gov/econ/susb/data/2008/us_state_totals_2008.xls
9 http://bjs.ojp.usdoj.gov/content/pub/pdf/csllea08.pdf
10 http://www.un.org/apps/news/story.asp?NewsID=38957
11 http://www.scip.org/
12 http://poole.ncsu.edu/erm/ and http://www.ermsymposium.org/2012/index.php
13 http://www.nextgov.com/the_basics/tb_20080623_2687.php
14 http://www.nonprofitrisk.org/
15 Lloyds of London. Under Attack: Global Business and the Threat of Political Violence.
http://www.lloyds.com/News-and-Insight/Risk-Insight/Reports/Terrorism/Threat-of-Political-Violence
16 Ernst and Young. 2011 Information Security Survey. http://www.ey.com/GL/en/Services/Advisory/2011-Global-Information-Security-Survey---Into-the-cloud--out-of-the-fog and Deloitte. Cyber Crime: A Clear and Present Danger.
http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf
17 Deloitte. Two Year Pandemic Preparedness Survey. http://www.deloitte.com/assets/Dcom-Turkey/Local%20Assets/Documents/turkey_en-lshc-yeartwopandemicsurvey130307.pdf
18 World Economic Forum/Wharton Business School. Global Risks 2011. http://riskreport.weforum.org/ and Aon Risk. Global Risk Management Survey. http://www.aon.com/risk-services/thought-leadership/reportspubs_2011_grms.jsp
19 Private communication with MPA alum working at Booz, Allen, Hamilton in cybersecurity who also has a National Guard billet in cybersecurity.
20 http://csis.org/publication/prepublication-a-human-capital-crisis-in-cyber security
21 http://www.bls.gov/news.release/ecopro.t03.htm
22 http://www.bls.gov/news.release/ecopro.t05.htm
23 http://www.bls.gov/oco/oco20016.htm
24 http://www.bls.gov/oco/oco20016.htm

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 describe their specific employment needs. If letters from employers support the program, they may be **appended** at the end of this form. As appropriate, address how the program will respond to evolving federal policy on the "gainful employment" of graduates of certificate programs whose students are eligible for federal student assistance.

Multiple federal, state and local agencies, as well as private sector industry, have long-term needs for properly trained employees in the area of homeland and cybersecurity. The certificate program will prepare professionals in several of the areas identified in section h)(1) above. Students are expected to be drawn from and return to these fields, including the following (with occupational codes from O*NET)

11-9161	Emergency Management Directors
11-9199.07	Security Managers
15-1122	Information Security Analysts

Students in the certificate program will have access to career services support from the Rockefeller College. This office will follow up with graduates for gainful employment information. Currently the office of Internships and Career Services collects this data on Master of Public Administration graduates.

Employer	Need: Projected positions	
	In initial year	In fifth year

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.*

Education in Homeland Security

Institution	Program Title	Degree	Enrollment
Elmira College	MS in Emergency-Disaster Preparedness Management	MS	Program is on hiatus, currently 2 students are finishing
John Jay College	MS in Protection Management MPA concentration in homeland security	MS, MPA	MS 39 MPA738
Long Island University	Homeland Security Management (M.S. and advanced Certificate Program)	MS	Not responsive to requests for information
Mercy College	MS in Cybersecurity	MS	Not responsive to requests for information
Metropolitan College of New York	Emergency and Disaster Management (M.P.A.)	MPA	37

New York Institute of Technology	MS in Information, Network, and Computer Security	MS	Not responsive to requests for information
New York University-Polytechnic	MS in Cybersecurity	MS	101
Rochester institute of Technology	MS in Computing Security and Information Assurance	MS	32
Syracuse University, Institute for National Security and Counterterrorism	National Security and Counterterrorism Law (Certificate, open only to Law students), Advanced Study in Security Studies (Certificate), Advanced Study in Postconflict Reconstruction (Certificate)	Cert	Consider enrollment information to be proprietary.
Utica College	Cybersecurity-Intelligence and Forensics (M.S.), Economic Crime and Fraud Management (M.B.A.), Economic Crime Management (M.S.)	MS, MBA, MS	MS 286 MBA 107 MS 69

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 was not built in consultation with other campuses. However, it was built in collaboration with UAlbany's College of Computing and Information and the School of Criminal Justice. The UAlbany School of Business was also consulted in regards to the program.

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

No concerns were expressed.

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 Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity are as follows:

- Official transcripts of all graduate and undergraduate work to date
- Proof of a baccalaureate or graduate degree from academic institution(s) where degree was earned (an official English translation should be provided if the original is not in English);
- Official transcripts from academic institution(s) where degree was earned (an official English translation should be provided if the original is not in English);
- A 1 to 2 page statement of background and goals;
- Evidence of proficiency in English for international applicants; and
- A completed application and fee.

These admission requirements are the same as all graduate certificate programs in Rockefeller College.

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

There will be no exceptions to these requirements.

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

The University at Albany has a demonstrated commitment to promoting diversity and inclusiveness among its student body, faculty, and staff. The Director of Graduate Recruitment and Admissions for the Rockefeller College will conduct targeted outreach to persons from historically underrepresented groups to encourage them to apply to the program. The College has participated in a number of Idealist Graduate Fairs where members of underrepresented groups often participate (particularly in New York, Chicago, and Washington). While no individual will be given preferential treatment for admission to the program, all persons will have equal access to the program and available resources. In order to increase recruitment of persons from historically underrepresented groups, Rockefeller College is in the process of joining the Public Policy and International Affairs (PPIA) program) which is a not-for-profit that has been supporting efforts to increase diversity in public service for over 30 years.

2.5. Academic and Other Support Services

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

Upon acceptance into the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity program, every student will be assigned an academic advisor. Typically, students will be initially assigned to the program director who will help the student decide what track and electives best fits his or her professional interests. As students take courses and meet faculty, many will choose to select a new advisor. To change advisors, the student should secure the agreement of another faculty member to serve as the new advisor and then notify the program director who will execute the change in the *myUAlbany* information system and record it in the student's records and in program documents.

Advisors are expected to monitor the student's progress and to ensure that the student complies with all procedural requirements in a timely manner. At a minimum, these duties include helping the student select courses, providing the student with an Advisor Verification Number (AVN) to permit registration via the *myUAlbany* webpage each semester, advising the student on other academic matters, discussing post-graduation career plans and writing letters of recommendation. The advisor will also assist the student in the completion of the Completed Degree Program (CDP) sheet, and other academic documents, as appropriate. The CDP sheet, which is a standard form for all certificate programs in Rockefeller College, is a final document outlining how the student has met the requirements of the program. During an in-person meeting, the sheet should be completed and signed by the student and the student's advisor. This must be done by the end of the fifth week of the student's last semester in the program. The CDP sheet is used by the director of graduate student services to review the student's credentials for graduation.

At the end of each semester, the program director, affiliated faculty who serve as academic advisors and relevant Rockefeller College staff will meet to review the progress and standing of all EHC certificate students. Students who are not making adequate progress will receive notification from the program director and receive additional counseling to identify and address problems. Students who do not maintain a 3.0 average will be placed on academic probation. Those who are unable to bring their average up to this threshold within one year will be administratively withdrawn from the program.

The certificate program must be completed within six years of the time a student is admitted into the program. While there is no continuous registration requirement, students who choose not to enroll for a semester (or more) do not have access to many services and they are unable to defer the repayment of prior college loans or qualify for financial aid.

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**.

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 learning objectives of the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity will be assessed on a bi-annual basis for the first year and a half after the program is initiated, with the first assessment completed in December 2015. One core course per semester will be assessed to determine if student learning outcomes are being met. After this initial assessment cycle, courses will be reviewed on an annual basis (courses will be assessed in the same order as they were initially assessed). After each course assessment, the committee of affiliated faculty will determine if additional assessment of the core courses is needed. Additional assessment would be required if it was determined during the initial assessment that the learning objectives were not being met and changes to the course were recommended. If it is determined that an additional assessment is needed, this would take place the following the semester in which the class was taught. If it is determined that no additional assessments are immediately needed, the annual assessment of each core course (one per year) will be continued according to schedule. At this time, elective courses will be assessed (one per year).

The attached curricular map lists the learning objectives of the EHC certificate program, the corresponding courses in which these objectives are met, and how the student learning outcomes are assessed. In each case, examinations and major assignments will be used to determine if the student learning outcomes were met. If student learning outcomes have not been met, it will be noted on this form.

Section 3. Sample Program Schedule and Curriculum

Complete the **SUNY Program Schedule for Certificate and Advanced Certificate Programs** to show how a typical student may progress through the program.

NOTE: *For a graduate advanced certificate program, the **SUNY Sample Program Schedule for Certificate and Advanced Certificate Programs** must include all curriculum requirements. The program is **not required** to conform with the program expectations from Part 52.2(c)(8) through (10) of the Regulations of the Commissioner of Education.*

> **a)** If the program has fewer than 24 credit hours, or 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.*

The Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity requires the completion of a minimum of 16 credit hours. The program will be offered on a traditional semester based schedule with normal time to completion being one year. Students who are enrolled at least half-time (six credit hours) in the program may be eligible for financial aid. This includes students who take classes during the traditional academic year (fall and spring semesters) as well as during the summer session.

> **b)** For each existing course that is part of the proposed undergraduate certificate or the graduate advanced certificate, append, at the end of this form, a catalog description.

> **c)** For **each new course** in the certificate or advanced certificate program, **append a syllabus** at the end of this document.

No new courses will be taught as part of this program.

> **d)** 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.

N/A

SUNY Sample Program Schedule for Certificate and Advanced Certificate Programs

Program/Track Title and Award: <u>Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity</u>

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. **Complete all columns that apply to a course.**

Track: Emergency Preparedness

Fall 1:

Course Number & Title	Credits	New (X)	Co/Prerequisites
PAD 557 - Intelligence Analysis for Homeland Security	4		
PAD 555 - Disaster, Crisis, and Emergency Management and Policy	4		
PAD 546 - Homeland Security Risk Analysis and Risk Management	4		
Term credit totals:	12		

Spring 1:

Course Number & Title	Credits	New (x)	Co/Prerequisites
PAD 553 - Topics in Homeland Security and Terrorism	4		
PAD 559 - Homeland Security: Building Preparedness Capabilities	4		
Term credit totals:	8		

Program Totals (in credits): | **Total Credits: 20**

Track: Homeland Security

Fall 1:

Course Number & Title	Credits	New (X)	Co/Prerequisites
PAD 557 - Intelligence Analysis for Homeland Security	4		
PAD 554 - Political Violence, Insurgency, and Terrorism	4		
PAD 556 – Homeland Security Intelligence	4		
Term credit totals:	12		

Spring 1:

Course Number & Title	Credits	New (x)	Co/Prerequisites
PAD 558 - Intelligence & US National Security Policymaking	4		
PAD 559 - Homeland Security: Building Preparedness Capabilities	4		
Term credit totals:	8		

Program Totals (in credits): | **Total Credits: 20**

16

Track: Cybersecurity

Fall 1:

Course Number & Title	Credits	New (X)	Co/Prerequisites
PAD 557 - Intelligence Analysis for Homeland Security	4		
PAD 545 - Principles and Practices of Cybersecurity	4		
PAD 546 - Homeland Security Risk Analysis and Risk Management	4		
Term credit totals:	12		

Spring 1:

Course Number & Title	Credits	New (x)	Co/Prerequisites
PAD 585 - Information Technology and Homeland Security	4		
PAD 550 - Foundations of Government Information Strategy and Management	4		
Term credit totals:	8		

Program Totals (in credits):	Total Credits: 20

17

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 Part 55.2(b) of the Regulations of the Commissioner of Education.

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

A full-time faculty member in the Rockefeller College at the University at Albany, in addition to significant research and service responsibilities, typically carries a teaching load of two graduate courses per term, plus dissertation research supervision of one to four doctoral students.

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.

18

(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					
*R. Karl Rethemeyer, Associate Professor & Program Director	5%	PAD 637 – Social and Organizational Networks	PhD – Harvard University	Public Policy	
Victor Asal, Associate Professor	10%	PAD 554 (POS 554) – Political Violence, Insurgency, and Terrorism PAD 625 (POS 626) – Bargaining and Negotiation POS 566 – Ethnic Conflict POS 567 – Contentious Politics: Theory and Research	PhD – University of Maryland	Government and Politics	
Kathleen Deloughery, Assistant Professor	10%	PAD 554 (POS 554) – Political Violence, Insurgency, and Terrorism PAD 705 – Research Methods II	PhD – The Ohio State University	Economics	
Brian Nussbaum, Assistant Professor	75%	PAD 545 –	PhD – University at	Political Science	

19

(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.
		Principles and Practices of Cybersecurity PAD 546 – Homeland Security Risk Analysis and Risk Management	Albany		
Sharon Dawes, Associate Professor	5%	PAD 550 – Foundations of Government Information Strategy and Management	PhD – University at Albany	Public Administration & Policy	
Theresa Pardo, Associate Research Professor	5%	PAD 550 – Foundations of Government Information Strategy and Management	PhD – University at Albany	Information Science	
David Andersen, Distinguished Service Professor	5%	PAD 504 – Data Models, and Decisions I PAD 624 – Simulating Dynamic Systems	PhD – Sloan School of Management	Management	
John Rohrbaugh, Professor	5%	PAD 505 (POS 505) – Data, Models,	PhD – University of Colorado	Social Psychology	

20

(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.
		and Decisions II			
Mitch Abolafia, Professor	5%	PAD 636 – Cultural Analysis of Organizations PAD 610 – Organizational Theory and Behavior	PhD – Stony Brook University	Sociology	
Sanjay Goel, Associate Professor	5%	ITM 604 – Data Communications, Computer Networking and Computer Security	PhD - Rensselaer Polytechnic Institute	Mechanical Engineering	
George Berg, Associate Professor	5%	Various CCI courses	PhD – Northwestern University	Computer Science	
Part 2. Part-Time Faculty					
Steve Sin	10%	PAD 554 (POS 554) – Political Violence, Insurgency, and Terrorism	BA – University of Texas	Government	PhD expected May 2015 from the University at Albany, Senior Research Associate, National Center for Security & Preparedness
Rick Mathews	20%	PAD 555 (POS 555) – Disaster, Crisis, and Emergency Management and Policy PAD 559 –	MS – Indiana State University	Health and Safety (Administrative emphasis)	Director, National Center for Security and Preparedness

(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.
		Homeland Security: Building Preparedness Capabilities			
Bryan Haynes	10%	PAD 545 - Principles and Practices of Cybersecurity	MPA – University at Albany	Public Administration and Policy	Associate with Booz Allen Hamilton and First Lieutenant, Cyber Operations Officer with the New York Air National Guard
Junesoo Lee	10%	PAD 505 – Data Models and Decision II	PhD – University at Albany	Public Administration and Policy	
James Steiner, Public Service Professor	100%	PAD 556 – Homeland Security Intelligence PAD 557 – Intelligence Analysis for Homeland Security PAD 558 – Intelligence & US National Security Policymaking PAD 559 – Homeland Security: Building Preparedness Capabilities	PhD – Georgetown University	Economics	Professional experience includes: Intelligence Advisor to the Director of New York State's Office of Homeland Security; senior advisor to the Undersecretary for Intelligence at DHS; over 30 years at the CIA
F. David Sheppard, Public Service	100%	PAD 553 –	MA – The United	Strategic Studies	Brigadier General; former director

(a)	(b)	(c)	(d)	(e)	(f)
Faculty Member Name and Title/Rank (Include and identify Program Director with an asterisk.)	**% of Time Dedicated to This Program**	**Program Courses Which May Be Taught (Number and Title)**	**Highest and Other Applicable Earned Degrees (include College or University)**	**Discipline(s) of Highest and Other Applicable Earned Degrees**	**Additional Qualifications: List related certifications, licenses and professional experience in field.**
Professor		Topics in Homeland Security and Terrorism	States Army War College		of the New York State Office of Homeland Security
Part 3. Faculty To-Be-Hired (List as TBH1, TBH2, etc., and provide title/rank and expected hiring date.)					

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.

The Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity does not require any major investments. As discussed above, the core courses are already regularly taught in the Department of Public Administration and Policy for the MPA program as a result, in part, of funding from NYSUNY 2020. New faculty in the Department of Public Administration and Policy and the Informatics Department, College of Computing and Information have already been hired.

b) Complete the five-year SUNY Program Expenses Table, below, consistent with the resource plan summary. Enter the anticipated <u>academic years</u> 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.

This program is funded using resources allocated by the University at Albany through the NYSUNY 2020 program.

SUNY Program Expenses Table
(OPTION: You can paste an <u>Excel version</u> of this schedule AFTER this sentence, and delete the table below.)

Program Expense Categories	Expenses (in dollars)					
	Before Start	2015-2016	2016-2017	2017-2018	2018-2019	2019-2020
(a) Personnel (including faculty and all others)	0	270,000	270,000	270,000	270,000	270,000
(b) Library	0	0	0	0	0	0
(c) Equipment	0	0	0	0	0	0
(d) Laboratories	0	0	0	0	0	0
(e) Supplies	0	0	0	0	0	0
(f) Capital Expenses	0	0	0	0	0	0
(g) Other (Marketing):	20,000	15,000	0	0	0	0
Other (faculty start-up)`	100,000					
Other (online course re-fits)	15,000	27,500				
(h) Sum of Rows Above	**135,000**	**312,500**	**270,000**	**270,000**	**270,000**	**270,000**

Section 6. Library Resources

NOTE: This section does not apply to certificate or advanced certificate programs.

Section 7. External Evaluation

NOTE: This section does not apply to certificate or advanced certificate programs.

Section 8. Institutional Response to External Evaluator Reports

NOTE: This section does not apply to certificate or advanced certificate programs.

Section 9. SUNY Undergraduate Transfer

NOTE: This section does not apply to certificate or advanced certificate 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? [ ] No   [X] 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? [ ] No   [X] Yes

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

NOTE: This section does not apply to certificate or advanced certificate programs.

List of Appended Items

Appended Items: Materials required in selected items in Sections 1 through 5 and Section 10 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 external standards	Section 2.3, Item (e)
	For programs leading to licensure in selected professions for which the SED Office of the Professions (OP) requires a specialized form, if required by OP	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)
1	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
2	For all programs, a catalog description for each existing course that is part of the proposed program	Section 3, Item (b)
	For all programs, syllabi for all new courses in the proposed program	Section 3, Item (c)
	For programs requiring external instruction, *External Instruction Form* and documentation required on that form	Section 3, Item (d)

	For programs that will depend on new faculty, position descriptions or announcements for faculty to-be-hired	Section 4, Item (b)
3	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

Appendix 1 – Curricular Map

	Public Administration – Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity					
	Learning Objectives	**Course or Level of Assessment**	**How Assessed**	**Date of Assessment**	**Noteworthy Results**	**Changes / Planned Changes**
1	Students will understand the basic analytic, methodological, and technical skills for analyzing homeland security and cybersecurity issues and the forces affecting flows of information, intelligence, and situational awareness. Extensive time is devoted to learning and using structured analytic techniques through student-led analytic exercises on terrorism and major crimes.	PAD 557	Final project	Fall 2015		
2	The student will understand why political violence is used, the forms it takes, those that use it, and how its targets' respond to it. The student will also understand the origin, nature, and impact of terrorism and the frameworks for understanding counterterrorism and counterinsurgency. Students will write in support of and against leading arguments in the field.	PAD 554 (POS 554)	Research paper	Spring 2016		
3	The student will understand the interaction between social, technical, policy, and management factors that affect the creation and management of secure cyber infrastructure. This includes the role of domestic criminal justice, intelligence agencies, private-sector infrastructure owners, and authorities with responsibility for responding to cyber attacks and the institutional frameworks within which homeland security and cybersecurity exist.	PAD 545	Research paper	Fall 2016		
4	The student will understand the policy frameworks that govern emergency response in the US and the institutional frameworks within which emergency response in the US operates.	PAD 555 (POS 555)	Research paper	Spring 2017		

Appendix 2 - Catalog Descriptions for Existing Courses

PAD 504 Data, Models, and Decisions I (4)
Introduction to computer-based tools for planning, policy analysis, and decision making. Topics include administrative and policy models in spreadsheets, dynamic models in difference equations and spreadsheets, making decisions with multiple criteria, resource allocation, probability and decision trees, data bases and information management, and telecommunications in local networks and the Internet. Prerequisites: Familiarity with word processing on either IBM or Macintosh platforms.

PAD 505 (POS 505) Data, Models, and Decisions II (4)
Basic introduction to statistical methods and tests. Specific course topics include measurement, probability, distribution, tables and graphs, estimation and hypothesis testing, and linear models. Emphasis is placed on interpreting and presenting statistical outputs, including reports generated by computer programs. Prerequisite: Graduate standing.

PAD 517 (POS 517) Empirical Data Analysis (4)
Introduction to a variety of data-analysis techniques ranging in complexity from simple table construction and interpretation to causal analysis. Within this range are coding, scale and index construction, multidimensional scaling, levels of measurement, measures of association, correlation and regression, panel and cohort analysis, and Markov chains. Introduction to computer technology and functional software. Basic competence in statistics necessary. Prerequisite: One course in statistics or consent of instructor.

PAD 518 (POS 518) Regression Analysis (4)
This course will give students familiarity with multivariate regression analysis, including Ordinary Least Squares and other regression methods. Prerequisites: POS 517 or PAD 505 or Pub 505 or equivalent.

PAD 545 Principles and Practices of Cyber Security (4)
This course provides a broad introduction to cyber security and the way in which cyber security is viewed, studied, or executed by professionals in industry, government, the military, and academia. For students that approach the topic from a policy or management perspective, this class will enhance your understanding of the interaction between social, technical, policy, and management factors that affect the creation and management of secure cyber infrastructure. A brief introduction to the technical side of cyber security will be provided. The course will offer technically advanced students an opportunity to better understand the management, policy, and political equities involved in cyber security. Students approaching the subject from either the technical or policy/management perspectives will be equipped to take a more advanced technical courses in a multitude of disciplines that make up cyber security. Prerequisites: PAD 554 or permission of instructor.

PAD 546 Homeland Security Risk Analysis and Risk Management (4)
This course looks at the various risks that homeland security professionals and researchers are forced to grapple with, including the various threats, vulnerabilities and consequences associated with these risks. It examines important homeland security policy areas through a risk analysis framework, with an emphasis on issues like infrastructure protection and resilience, cybersecurity, terrorism, and the implications of catastrophic disasters (both naturally occurring and human-caused disasters). In each of the policy areas of concern, the class will discuss both the risks that exist, but also risk mitigation strategies; including the building of capabilities for preparedness, prevention, protection, response, and recovery. Prerequisites: PAD 554 or permission of instructor.

PAD 550 Foundations of Government Information Strategy and Management (4)
Introduces the interaction of policy, management, and information technology in the design, operation, and evaluation of government operations and public services. Relies heavily on case studies to illustrate how these

domains play out in multiple settings and across sectors-public, private, and not-for-profit. Prerequisites: PAD 500 and PAD 506, and Permission of Instructor.

PAD 551 (CRJ 648) Terrorism, Public Security, and Law Enforcement (3)
This course reviews the role of domestic law enforcement in homeland security, including the prevention of and response to terrorism. Consideration of strategic issues that arise with respect to specific forms of terrorist threats, and of managerial issues, including the collection, analysis, and dissemination of intelligence, risk assessment and resource allocation, intergovernmental and interagency cooperation and conflict, and investigative authority and civil liberties.

PAD 553 Topics in Homeland Security and Terrorism (4)
This course examines an array of topics related to homeland security, terrorism, responses to terrorism, and the role of terrorism in public policy problems. Depending on the semester, the course will focus on a subset of issues in this field and may include both substantive and methodological topics relevant to the study of homeland security and terrorism. Course may be repeated with topic change.

PAD 554 (POS 554) Political Violence, Insurgency and Terrorism (4)
This course examines the relationships among, and differences between the following activities in the international political system: political violence, insurgency, and terrorism. The course will include a consideration of the causes of these activities, their effects on national and international politics, and an evaluation of governmental responses to them.

PAD 555 (POS 555) Disaster, Crisis and Emergency Management and Policy (4)
Study of the policies designed to prepare for, respond to, mitigate, and recover from natural and technological disasters, accidents, or terrorist attacks. Surveys government, non profit, and private sector activities in emergency and crisis management and policy.

PAD 556 Homeland Security Intelligence (4)
This course examines Homeland Security Intelligence at the Federal, State, and local levels. We begin with an overview of the US foreign intelligence community, its mission, history, structure, and capabilities. We examine how this community's composition and structure have changed as its mission was fundamentally altered twice, first with the end of the Cold War and then with the rise if terrorism. Next, we look at the capabilities of new producers of terrorism related intelligence at federal law enforcement agencies and at the Department of Homeland Security. The main thrust of the course is intelligence at the State and local levels. The federal government has worked with the states to create significant intelligence capabilities outside the beltway since the events of 9/11/2001. This course identifies and discusses the State and local customers for homeland security intelligence and examines the degree to which these intelligence requirements are being met.

PAD 557 Intelligence Analysis for Homeland Security (4)
This course provides instruction in conducting intelligence analysis, with emphasis on homeland security issues at the State and local levels. After an overview of the history and structure of the US foreign intelligence community, we review the fundamentals of intelligence analysis tradecraft as practiced within the CIA and other federal intelligence agencies. Extensive time is devoted to learning and using structured analytic techniques through student-led analytic exercises on terrorism and major crimes.

PAD 558 Intelligence & US National Security Policymaking (4)
This seminar examines the role of intelligence in the formulation and implementation of US foreign policy. Through critical analysis and case studies, students will develop techniques to increase intelligence's contribution to policy deliberations while ensuring that it does not prescribe policy. The course will assess the most

appropriate role for the CIA and the Intelligence Community in supporting this executive branch process. After an overview of the CIA, its functions, structure, and capabilities. We review the US foreign policy process, key players, and institutional bias. The bulk of the course is devoted to a series of mock intelligence and policy meetings on the Bosnia, Kosovo, Afghanistan, and Iraq crises to critically analyze the CIA's proper role in supporting the policy process.

PAD 559 Homeland Security: Building Preparedness Capabilities (4)
The short but significant history of the creation of the U.S. Department of Homeland Security (DHS) will serve as the starting point for this course which will provide a comprehensive and functional approach to understanding this department and its role. The preponderance of time will be spent in developing an understanding of the nation's effort, led by DHS to develop preparedness capabilities to prevent, protect from, respond to, and recover from high consequence events caused by acts of terrorism, natural disasters, and accidents. The course will rely heavily upon scenario-based activities and case studies to guide the student through the DHS maze and the nation's preparedness efforts at the federal, state, and local levels.

PAD 583 (POS 583) Global Governance (4)
The organization of world politics in the context of globalization. Overview of international organizations such as the United Nations and regional organizations such as the European Union. Examination of the historical and current international legal frameworks. Analysis of international cooperation beyond the confines of formal organizational structures with particular emphasis on international regimes, institutions and norms that govern state practices in particular issue areas – from trade and weapons proliferations to the environment and refugees. Also examines transnational relations of non-state actors such as nongovernmental organizations (NGOs) and multinational corporations as well as transgovernmental relations of sub-national governments and government agencies that shape policymaking at a global level.

PAD 585 (POS 585, INF 585) IT and Homeland Security (4)
This course examines the political, legal and policy aspects of the use of information technologies by the US Department of Homeland Security (DHS), non-technological dimensions of information collection, use and management and the use of technologies other than computing in the homeland security domain. The course is focused on information technology use by the US federal government but will also examine state and local governments and other countries as well as international issues such as information sharing and international technical standards.

PAD 610 Organizational Theory and Behavior (4)
This course uses social science theories and methods to understand human behavior in organizations. It explores such important areas as decision-making, perception, communication, group dynamics, and such managerial issues as organizational politics, organizational culture, and organizational change. Students employ case studies and exercises to develop skills in organizational analysis.

PAD 624 (ITM 624) Business Dynamics: Simulation Modeling for Decision-Making (3-4)
Explores the use of computer models to understand, diagnose, and experiment with organizational policy and design options. Students will learn about simulation-based analysis, employ a simulation tool, and apply their knowledge to problems of current importance. Prerequisites: Itm 520, ITM 522, or PAD 504 or consent of the instructor.

PAD 625 (POS 626) Bargaining and Negotiation (4)
Survey of theories of bargaining and negotiation, with emphasis on the use of analytic and quantitative methods to help understand and facilitate negotiation processes. Extensive use of simulation, exercises, role playing, and cases.

PAD 636 Cultural Analysis of Organization (4)
Exploration of the cultural approach to organizational analysis: theory and methods from anthropology, sociology, and history that focus on the subjective experience of organization members. Students complete a study in which these theories and methods are applied to a public, private or non-profit organization. Prerequisite: Graduate standing.

PAD 637 Social and Organizational Networks in Public Policy, Management, and Service Delivery: Theory, Methods, and Analysis (4)
The concept of "network" has become central to many discussions of public policy, management, and service delivery but is rarely studied systematically. This course is designed to explore the theoretical underpinnings of network analysis, introduce basic network analytic methods, and examine and compare insights gained through network analysis with other forms of analysis. Prerequisites: Completion of required statistical courses for the Master's or Ph.D. program; permission of instructor.

PAD 705 Research Methods II (4)
Intermediate course in specific research techniques and tools of analysis; qualitative and quantitative techniques of analysis addressed. Prerequisite: PAD 704.

POS 550 Field Seminar in Comparative Political Systems (4)
Survey of the basic substantive, methodological, and normative concerns of contemporary scholars of comparative political systems. Offered jointly by the faculty in comparative politics.

POS 566 Ethnic Conflict (4)
Since the end of the cold war, ethnicity has served as a key source of identity conflict. This course will examine on the domestic and international aspects of ethnic conflict and the Possibilities for management offered by a variety of institutional arrangements and international intervention.

POS 567 - Contentious Politics: Theory and Research (4)
Contentious politics focuses on politics outside of the normal boundaries of institutionalized politics. From protests to riots and revolutions, contentious politics have often led to major shifts in domestic political orders. This course will explore key theories and methods in the study of contentious politics.

POS 570 Field Seminar in International Political Systems (4)
A survey of the substantive, methodological, and normative concerns of contemporary scholars of international relations. Offered jointly by the faculty in international relations as the basic foundation course.

POS 582 Global Security (4)
An introduction to competing theoretical approaches to the study of international security that considers alternative conceptual approaches, such as societal security and human security. Reviews the evolution of nuclear deterrence and explores issues of nuclear, chemical and biological weapons proliferation, asymmetric warfare and homeland security. Prerequisite(s): As specified for M.A. and Ph.D. students.

IST 532 Terrorism, Public Security, and Information Analysis (3)
This course discusses information technologies available to assist in intelligence analysis, as well as defensive tools used to combat cyberterrorism and protect our information-based infrastructure. Techniques include advanced information retrieval, summarization, and linking, data analysis and data mining technologies. Legal and ethical issues related to intelligence gathering and monitoring will also be included.

ITM 604 Data Communications, Computer Networking and Computer Security (3)
This class introduces communications and networking concepts, including types of networks, data/signal transmission, basic ideas such as error control and multiplexing, as well as the costs and benefits of different

wired and wireless media and communications hardware. It covers network topologies, the OSI/Internet models, associated protocols (TCP/IP), network architectures, and network routing and switching. Information security concepts are introduced, including common risks to information systems and their controls. Specific areas covered include wireless security, application security, password security and Access control, cryptography and secure electronic commerce (PKI, digital certification, digital signatures, and other electronic authentication), intrusion detection/prevention, incident response, and computer forensics. Students also perform a risk analysis exercise using a real-world case and learn to develop information security policy. Prerequisite: ITM 522 or permission of instructor.

ITM 640 Information Security Risk Assessment (3)

This course provides students with an introduction to the field of information security risk assessment. Initially, the students will be introduced to basic definitions and nomenclature in the area of security assessment. Thereafter they will be taught different approaches for assessment of risk. The course will incorporate cases in risk analysis derived from state and law enforcement agencies. Students will learn how to use a risk analysis matrix for performing both quantitative and qualitative risk analysis. As part of the course the students learn of the different threats that they need to incorporate in their risk analysis matrices.

ITM 641 Security Policies (3)

This course provides students with an introduction to information security policies. Students will be introduced to sociological and psychological issues in policy implementation in general and then provided with a focused dialogue on information security specific policies. The class discusses the entire lifecycle of policy creation and enactment and presents students with issue specific policies in different domains of security. The structure of the policy is also discussed to assist the students in design and modification of policies. Several examples from different domains are incorporated in the curriculum to assist students to learn in context of real life situations.

ITM 642 Computer Forensics (3)

This course prepares students to conduct a computer forensics investigation as prescribed by the National Institute of Justice (NIJ). Students will be introduced to computer forensics concepts, as well as techniques for identifying, collecting, preserving and triaging digital evidence consistent with industry standards and best practices. Students will become familiar with assorted hardware and software utilized by computer forensic practitioners

ITM 643 Incident Handling (3)

The course primarily involves management of computer security incidents, including detailing different types of incidents, identification, preparation, and analysis of incidents; as well as gathering of evidence, recovery and follow-up to computer security incidents.

ITM 644 Introduction to Information & Cyber Security (3)

In this class, vulnerabilities of computer networks and techniques for protecting networks and data are discussed. Basic elements of symmetric and asymmetric cryptography, secure e-commerce, involving secure transmission, authentication, digital signatures, digital certificates and Public Key Infrastructure (PKI) is presented. Issues in privacy and piracy are also discussed where students study and debate controversial topics such as media piracy and government surveillance.

ITM 645 Psychology & Information Security (3)

This course provides students with an appreciation for and understanding of the psychological processes that impact information security. Three broad themes are covered. The first explores the psychology of the attacker, and examines the motivation and techniques of cyber criminals and hackers. The second theme stresses the importance of the user in the success of security systems. Students will be introduced to basic perceptual, cognitive, and motivational processes and biases that compromise security and increase vulnerability to attacks. The third theme examines how humans interact with machines and technology and how this interaction affects security in organizations.

ITM 646 Mathematical Models for Information Security (3)

This course teaches students to navigate sections of classical mathematics and computer science used to construct mathematical models of information security. This course will help students understand the need for mathematical models in different security paradigms along with the essential definitions, concepts and results for developing the models. The course will also help students figure out the limitations of the mathematical model: its strengths and weaknesses, and, consequently, its application to practical problems. The student will know what specific areas of mathematics and computer science will be necessary for the problems at hand and where further investigation is required.

ITM 647 Security Implementation

This course will teach students how to implement security in networks. Students learn how to harden their information security environment and set up secure infrastructure. The course covers both wired and wireless network security, database security, and general computer security practices.

ITM 691 Field Study in Information Technology Management (3)

Field projects are conducted by students under faculty supervision in a variety of business and not-for-profit organizations. The projects provide students with an opportunity to apply and further develop their skills in information technology management. Must be repeated for 3 credits. Prerequisites: ITM 522 and permission of the department chairperson.

CRJ 504 Applied Statistics I (3)

Introduction to statistical techniques appropriate for use in the criminal justice field. Descriptive statistics; scales of measurement; measure of central tendency, variability, and association. Introduction to statistical inference including sampling distributions and tests of significance.

CRJ 505 MA Research Design (3)

This course provides an introduction to methods of research used in criminal justice and social sciences. Major topics include the logic of social inquiry, causality, and conceptualization; sampling theory; data collection and measurement; and research design. The primary objectives of this course are: 1) to help students be informed consumers of contemporary criminal justice research and 2) to enable students to initiate and execute worthwhile research projects of their own. MA students only or with permission of the instructor.

CSI 416/516 Computer Communication Networks (3)

Introduction to computer communication networks. Equal emphasis on all layers of the ISO reference model and the TCP/IP protocol suite. Topics include physical networks, sliding window protocols, remote procedure call, routing, naming and addressing, security, authentication, performance, and applications. Prerequisite(s): I CSI 402 and A Mat 367. Normally offered fall semester only.

CSI 424/524 Information Security (3)

This course covers the broad spectrum of technical issues surrounding computer security and intrusion detection. Topics considered include: viruses, worms, host- and network-based vulnerabilities and countermeasures, database security, intrusion detection, and privacy and legal issues. Facilities for securing hosts and limiting vulnerability are also discussed. Unlike in a systems administration class, detailed operational issues are not discussed. Prerequisite(s): I CSI 402 or I CSI 400.

CSI 426/526 Cryptography (3)

The making of ciphers to encode information is the subject of cryptography. This course covers the field from its origins in early historic times through its most up-to-date implementations and uses in digital computers. Various ciphers will be shown and their security assessed. This latter is known as cryptanalysis – the attempt to break a cipher in order to read the underlying message. The course will emphasize how cryptography and cryptanalysis

are intimately related, and how the arms race between the two has motivated progress throughout their history. Prerequisite(s): I CSI 333 and co-registration in I CSI 403.

CSI 628 Cryptographic Protocols (3)

This course is on analyzing cryptographic protocols on security issues. The emphasis will be on formal methods, i.e., logically analyzing the protocols to establish the presence or absence of security flaws. The students will read and present latest cutting-edge literature and there will be a term project. Prerequisites: CSI 503 (or equivalent) as a co-requisite, departmental examination in Discrete Mathematics, CSI 524 or 526.

FOR 610 International Cyber Conflicts (3)

Cyber Security is an international problem where the perpetrators and victims of attacks may be in completely disparate locations. Cyber attacks have morphed from cyber crime and amateur display of prowess into cyber warfare and espionage among nations. While the issues are international there is little consensus on how to investigate them, create universally acceptable norms, and create international laws across multiple countries to manage them. This course discusses some of these sensitive issues regarding information security and cyber warfare. The hope is to improve understanding between professionals and students across countries in order to foster cooperation in resolving cyber conflicts. The class will include cases and discussions that will touch on the sensitive security related topics.

FOR 611 Supervisory Control And Data Acquisition (SCADA) Forensics (3)

Supervisory Control And Data Acquisition (SCADA) systems are computer systems controlling large-scale, industrial equipment, often underlying important infrastructural assets such as power plants, water distribution facilities, and communication networks. This class is intended to familiarize students with how to forensically investigate and secure SCADA system. Due to the nature and impact of SCADA systems on human lives they typically have more requirements than standard systems. Because SCADA systems are imbedded into critical infrastructure it is vital to understand the regulatory compliance and system governance associated with these systems. As recent events, both domestically and internationally, have demonstrated, SCADA forensics skills are increasingly important and in demand today. Prerequisites: R CRJ 281, A MAT 108, or equivalent; recommended B FOR 201 and 202.

FOR 613 Multimedia Forensics (3)

This course prepares students to conduct digital forensic examinations on multimedia evidence, specifically images, videos and audio files. The course builds student knowledge from the basics of multimedia types to being able to recognize anomalies in the files and identify file creation attributes. Students will learn how to examine multimedia files manually and through automated processes utilized by digital forensic tools. Students will prepare written reports outlining their findings of analysis, in a professionally acceptable manner, pursuant to administrative, civil and criminal legal proceedings. Graduate students will be expected to do extra or more advanced assignments. Prerequisites: R CRJ 281, A MAT 108, or equivalent; recommended B FOR 201 and 202.

INF 503 Advanced Networking and Security (3)

This course is designed to provide an advanced coverage of networking with a specific focus on network security and cryptography. Networking security is examined through a study of digital signatures and certificates, authentication protocols, and firewalls and key establishment and management. Also considered are security issues related to people's use of computer networks, communication channels, mobile devices, and the Internet. Also examined are new access control paradigms such as Java security and .NET security. (The programming experience will allow the course to include a hands-on security project). Prerequisite: Some programming.

INF 504 Advanced Systems and Security (3)

This course is designed to provide an advanced coverage of systems with a specific focus on cyber security. Engineered security is examined through the application and introduction to authentication protocols

and intrusion detection for Unix, Windows and databases and general software security. Also considered are security issues related to people's use of systems including policies and practices for password management and protecting privacy rights. Students also study options for maintaining business continuity in the event of a disruption of business operations. Security models such as Bell-LaPadula are introduced and studied. Specific case studies are used to highlight the choices that must be made to balance operational efficiency of business functions with protecting the business from the onslaught of security threats.
Prerequisite: Some programming.

INF 552 Computer and Network Security (3)
Theoretical, conceptual and practical aspects of computer and network security. The role of algorithms, systems, humans, software and hardware in computer and network vulnerabilities and defense. The two primary focuses of the course will be on the computer and networks, as centers of vulnerability and defense. The course will emphasize hands on analysis of security issues.
Prerequisite: INF 306 or background in cyber-security.

INF 553 Information Security and Privacy (3)
Security and Privacy issues in computer and networked systems. The role of systems, design, implementation, etc. on data security in digital systems. Case studies of those roles and how they affect both data security and vulnerability. The legal and ethical aspects of data security and privacy.
Prerequisites: INF 306 or background in cyber-security.

INF 554 Human Aspects of Cyber-security (3)
The roles of individuals, groups, organizations and governments in computer and network security. How the interactions of these with the technical nature of digital systems in many cases forms the core of vulnerabilities. The trade-offs between security and various measures of utility. Conflicting definitions of security at different levels (e.g. governmental v. individual). Societal measures and values of security. The course will feature case studies to explore many of these issues.
Prerequisite: INF 306 or background in cyber-security.

INF 555 Prevention and Protection Strategies in Cyber-security (3)
The role of security policies and design strategies to minimize security vulnerabilities in computer and networked systems. The affected areas range from the overall design of systems, networking protocols, operating systems and applications software on individual computers. The role of coding standards. End user education and role in security.
Prerequisite: INF 306 or background in cyber-security.

Appendix 3 - Distance Education Format Proposal

Distance Education Format Proposal
For A Proposed or Registered Program
Form 4

When a new or existing program is designed for a <u>distance education format</u>, which enables students to complete 50% or more of the course requirements at a distance, a campus Chief Executive Officer or Chief Academic Officer should submit a signed cover letter and this completed form to the SUNY Provost at <u>program.review@suny.edu</u>. According to MSCHE, the 50% standard includes only courses offered in their entirety via distance education, not courses utilizing mixed delivery methods. Also, MSCHE requires that the first two programs for which 50% or more is offered through distance education be submitted for Commission review and prior approval of a substantive change.

- All campuses must complete the following sections: Contact and Program Information, Section 1: Enrollment, Section 2: Program Information, and Part B: Program Specific Issues.

- Part A must be completed if the proposing campus has not previously submitted this form with a completed Part A: Institution-wide Issues, or has made significant changes to its institution-wide distance education operations since last completing Part A. This applies even if the institution has programs registered to be delivered at a distance.

Contact and Program Information
Institution's <u>6-digit SED Code</u>: 210500
Institution Name: University at Albany
Institution Address: 1400 Washington Ave., Albany, NY 12222
NYS Department of Labor/<u>Regents Region</u>: Capital Region
CEO or Designee: Robert J. Jones
CEO/Designee Signature: Date:

Chief Executive Officer or Designee 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.

Distance Education Contact Person Name and Title: R. Karl Rethemeyer, Interim Dean, Rockefeller College	
Telephone:518-442-5283	Email:
Program Title: Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity	<u>SED Program Code</u> (for existing programs):
Degree or Certificate Award: Graduate Certificate	<u>HEGIS Code</u>: 2102 Public Administration

Section 1: Enrollment

Anticipated enrollment in distance program: 10

Section 2: Program Information

a) **Term length** (in weeks) for the distance program: 15

b) Is this the same as term length for classroom program?   [   ] No   [X] Yes

c) How much "**instructional time**" is required per week per credit for a distance course in this program? (Do not include time spent on activities that would be done outside "class time," such as research, writing assignments, or chat rooms.)   **NOTE:** See <u>SUNY policy on credit/contact hours</u> and <u>SED guidance</u>.

The instructional time for the courses in the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity (EHC) program will be 170 minutes of class time per week per four credit course (e.g., the course meets once a week from 5:45pm to 8:35pm). This is the same instructional time as the vast majority of graduate courses currently offered by Rockefeller College at the University at Albany.

d) What proportion or percentage of the program will be offered in Distance Education format? Will students be able to complete 100 percent of the program online? If not, what proportion will be able to be completed online?

Students will be able to complete 100% of the program online. Students will have the option of taking courses in both online and offline (traditional face to face) formats.

e) What is the maximum number of students who would be enrolled in an online course section?

Online courses in the EHC program would adhere to the University at Albany standard operating procedure of capping classes at 25 students.

Part A: Institution-wide Issues: Submit Part A only for the **first** Distance Education program proposed by your institution using this form. SUNY and the State Education Department will keep this in a master file so that your institution will not need to resubmit it for each new proposed online program, **unless there are significant changes, such as a new platform**.

I.   ORGANIZATIONAL COMMITMENT

a) Describe your institution's planning process for Distance Education, including how the need for distance access was identified, the nature and size of the intended audiences, and the provisions for serving those audiences, including how each student's identity will be verified.

b) Describe your institution's resources for distance learning programs and its student and technical support services to ensure their effectiveness. What course management system does your institution use?

c) Describe how the institution trains faculty and supports them in developing and teaching online courses, including the pedagogical and communication strategies to function effectively. Describe the qualifications of those who train and/or assist faculty, or are otherwise responsible for online education.

d) If your institution uses courses or academic support services from ***another provider***, describe the process used (with faculty participation) to evaluate their quality, academic rigor, and suitability for the award of college credit and a degree or certificate.

e) Does your institution have a clear ***policy on ownership of course materials*** developed for its distance education courses? How is this policy shared with faculty and staff? ***NOTE:*** *You may refer to SUNY's statement on copyright and faculty ownership of instructional content, and/or faculty contract provisions.*

II.   LEARNER SUPPORT

a)   Describe how your institution provides distance students with ***clear information*** on:
- Program completion requirements
- The nature of the learning experience
- Any specific student background, knowledge, or technical skills needed
- Expectations of student participation and learning
- The nature of interactions among faculty and students in the courses.
- Any technical equipment or software required or recommended.

b)   Describe how your institution provides distance learners with adequate ***academic and administrative support***, including academic advisement, technical support, library and information services, and other student support services normally available on campus. Do program materials clearly define how students can access these support services?

c)   Describe how ***administrative processes*** such as admissions and registration are made available to distance students, and how program materials inform students how to access these services.

d)   What ***orientation*** opportunities and resources are available for students of distance learning?

Part B: Program-Specific Issues: Submit Part B for <u>each new request</u> to add Distance Education Format to a proposed or registered program.

III.   LEARNING DESIGN

a)   How does your institution ensure that the ***same academic standards and requirements*** are applied to the program on campus and through distance learning? If the curriculum in the Distance Education program differs from that of the on-ground program, please identify the differences.

Both the online and on campus programs were constructed by the same faculty group, which is comprised of primarily tenured and tenure-track faculty with input from highly experienced Public Service Professors (professors that are professionally rather than academically qualified to teach in the program. For instance, our faculty group includes a 33-year CIA veteran with a PhD and a former brigadier general with teaching experience at West Point.) The program <u>will not</u> be principally staffed by temporary faculty. Advising for all certificate students, whether online or on campus, will be handled by members of the faculty group.

With two exceptions, all courses offered online are offered on campus using the same syllabus with some modifications for online purposes (for instance, using online small groups rather than in-class small group discussions). The core cybersecurity and emergency preparedness courses, PAD 545 and PAD 555, were developed from origin as online courses (in-class courses based on the existing syllabus will be developed during the 2015 calendar year). Courses are of the same length and have the same assignments and examinations.

b)   Are the courses that make up the distance learning program offered in a sequence or configuration that allows ***timely completion of requirements***?

Yes. PAD 557, which is required of all students in the EHC program, will be taught both online and in a face-to-face format each academic year. In addition, the required course for each track (PAD 554, PAD 545 and PAD 555) will be offered online each academic year. Although all elective courses for each track will not be offered yearly, a sufficient number (at least 3) will be offered online each academic year to allow students to complete the certificate in one year. The sequence that the courses are offered each year will be carefully thought out to ensure that students have appropriate classes to choose from to complete the core and elective requirements.

c) How do faculty and others ensure that *the technological tools* used in the program are appropriate for the content and intended learning outcomes?

In the process of developing new courses, faculty members and staff will test technological tools in cooperation with the Course Management and Instructional Technology division of the University at Albany's Information Technology Services (ITS) and the UAlbany teaching and learning center (the Institute for Teaching, Learning and Academic Leadership, ITLAL). With the assistance of ITS and ITLAL, we will develop a standard training module for all public service professors, adjunct faculty and tenure track faculty using the technology for the first time. Rockefeller College has also received a distance learning grant from the UAlbany Provost's office that will support training of faculty and graduate students in synchronous and asynchronous distance learning. We anticipate that this grant will support fielding more elective courses in distance learning format, particularly in the EHC and proposed Master of International Affairs (MIA) programs.

d) How does the program provide for appropriate and flexible interaction between faculty and students, and among students?

Faculty members will be available to interact with students through a variety of means – in person during office hours or scheduled appointments, via telephone, and/or via the use of Adobe Connect (or similar software) or Skype for students who prefer face to face interaction but are unable to meet in person due to distance or some other limitation. The technology that will be used for the classes will also allow interaction between students and faculty and students and students through message boards and file sharing systems.

e) How do faculty teaching online courses verify that the student who registers in a distance education course or program is the same student who participates in and completes the course or program and receives the academic credit?

Faculty members will be required to abide by the University at Albany's ITS policy on identity access and management (available at https://wiki.albany.edu/display/public/askit/Identity+Access+and+Management+Policy). These policies ensure that the student who registers in a distance education program is the same student who participates in and completes the program and thus receives the academic credit. UAlbany students who participate in such classes are required to use secure login procedures for their online classes. Every student will be required to use the unique online identity (PIN, Albany ID, NetID) that is assigned to them by the University. A password is established by the student for the purpose of authenticating their assigned identity. PINS and passwords are confidential and must not be shared with anyone.

a) Distance learning programs are expected to produce the ***same learning outcomes*** as comparable classroom-based programs. How are these learning outcomes identified – in terms of knowledge, skills, or credentials – in course and program materials?

Distance learning courses will have learning objectives stated in course syllabi. The learning outcomes for these courses will be the same as equivalent courses taught in the traditional face to face classroom setting. These learning outcomes will be assessed according to the schedule provided in Form 2C and outlined in section V below.

b) Describe how the ***means chosen for assessing student learning*** in this program are appropriate to the content, learning design, technologies, and characteristics of the learners.

Courses will use examinations, written assignments, homework problem sets, group projects, and class participation as means of assessing student learning. These methods are commonly used throughout the College's other comparable programs.

V. PROGRAM EVALUATION

a) What process is in place to monitor and ***evaluate the effectiveness*** of this particular distance education program on a regular basis?

The distance education courses offered as part of the EHC program will be evaluated according to the same standards used to evaluate and asses all courses, including traditional classroom courses. The learning objectives of the core courses will be assessed on a bi-annual basis for the first two-years after the program is initiated by the homeland security program director. One core course per semester will be assessed to determine if student learning outcomes are being met. After this initial assessment cycle, courses will be reviewed on an annual basis (courses will be assessed in the same order as they were initially assessed). After each course assessment, the homeland security program chair will determine if additional assessment of the core courses is needed. Additional assessment would be required if it was determined during the initial assessment that the learning objectives were not being met and if changes to the course were recommended. If it is determined that an additional assessment is needed, this would take place the following semester in which the class was taught. If it is determined that no additional assessments are immediately needed, the annual assessment of each core course (one per year) will be continued according to schedule. Once the core courses have all be assessed positively, elective courses will be assessed (one per year).

b) How will the evaluation results be used for ***continuous program improvement***?
If it is determined that learning objectives are not being met in any of the EHC program courses, the program director would meet with all faculty responsible for teaching the course to determine how the content and delivery of the course material could be improved so that learning objectives are met. This would include comparison of course content to comparable courses both within the University at Albany and at similar programs in peer institutions. Should it be determined that the delivery of the material is not meeting expectations, faculty members would be required to seek training from the Course

Management and Instructional Technology division of the University at Albany's Information Technology Services (ITS) and the UAlbany teaching and learning center (the Institute for Teaching, Learning and Academic Leadership, ITLAL).

c) How will the evaluation process assure that the ***program results in learning outcomes appropriate to the rigor and breadth*** of the college degree or certificate awarded?

The director of the EHC program, in consultation with the dean of Rockefeller College, will review learning outcomes in conjunction with graduation statistics, average time-to-degree and student career placements (e.g., percent placed, average wage, field of specialization) compiled annually by the director of internships and career services. Emergency Preparedness, Homeland Security, and Cybersecurity alumni will also be regularly surveyed to determine career trajectories and how our programs could be altered to better equip our students for a competitive job environment.

VI. STUDENTS RESIDING OUTSIDE NEW YORK STATE

SUNY programs must comply with all "authorization to operate" regulations that are in place in other U.S. states where the institution has enrolled students or is otherwise active, based on each state's definitions.

a) What processes are in place to monitor the U.S. state of residency of students enrolled in any distance education course in this program while residing in their home state?

The University at Albany Graduate Admissions Office and the Office of the Registrar monitor and verify residency for all graduate students.

b) Federal regulations require institutions delivering courses by distance education to provide students or prospective students with contact information for filing complaints with the state approval or licensing entity in the student's state of residency and any other relevant state official or agency that would appropriately handle a student's complaint. What is the URL on your institution's website where contact information for filing complaints for students in this program is posted? ***NOTE:*** *Links to information for other states can be found at http://www.suny.edu/provost/dlo/dl_outofstate.cfm.*

http://www.albany.edu/graduatebulletin/requirements_student_complaints.htm

Version 2013-10-15

Distance Education Format Proposal
For A Proposed or Registered Program
Form 4

When a new or existing program is designed for a <u>distance education format</u>, which enables students to complete 50% or more of the course requirements at a distance, a campus Chief Executive Officer or Chief Academic Officer should submit a signed cover letter and this completed form to the SUNY Provost at <u>program.review@suny.edu</u>. According to MSCHE, the 50% standard includes only courses offered in their entirety via distance education, not courses utilizing mixed delivery methods. Also, MSCHE requires that the first two programs for which 50% or more is offered through distance education be submitted for Commission review and prior approval of a substantive change.

- All campuses must complete the following sections: Contact and Program Information, Section 1: Enrollment, Section 2: Program Information, and Part B: Program Specific Issues.

- Part A must be completed if the proposing campus has not previously submitted this form with a completed Part A: Institution-wide Issues, or has made significant changes to its institution-wide distance education operations since last completing Part A. This applies even if the institution has programs registered to be delivered at a distance.

Contact and Program Information Institution's <u>6-digit SED Code</u>: 210500
Institution Name: University at Albany
Institution Address: 1400 Washington Ave., Albany, NY 12222
NYS Department of Labor/<u>Regents Region</u>: Capital Region
CEO or Designee: Robert J. Jones
CEO/Designee Signature: Date:

Chief Executive Officer or Designee 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.

Distance Education Contact Person Name and Title: R. Karl Rethemeyer, Interim Dean, Rockefeller College	
Telephone:518-442-5283	Email:
Program Title: Emergency Preparedness, Homeland Security, and Cybersecurity	<u>SED Program Code</u> (for existing programs):
Degree or Certificate Award: Graduate Certificate	<u>HEGIS Code</u>: 2102 Public Administration

Section 1: Enrollment

Anticipated enrollment in distance program: 10

Initial Year: 2   Maximum by Year 3: 7

Section 2: Program Information

a) *Term length* (in weeks) for the distance program: 15

b) Is this the same as term length for classroom program?   [ ] No   [X] Yes

c) How much "*instructional time*" is required per week per credit for a distance course in this program? (Do not include time spent on activities that would be done outside "class time," such as research, writing assignments, or chat rooms.)   ***NOTE:*** *See SUNY policy on credit/contact hours and SED guidance.*

The instructional time for the courses in the Graduate Certificate in Emergency Preparedness, Homeland Security, and Cybersecurity (HCE) program will be 170 minutes of class time per week per four credit course (e.g., the course meets once a week from 5:45pm to 8:35pm). This is the same instructional time as the vast majority of graduate courses currently offered by Rockefeller College at the University at Albany.

d) What proportion or percentage of the program will be offered in Distance Education format? Will students be able to complete 100 percent of the program online? If not, what proportion will be able to be completed online?

Students will be able to complete 100% of the program online. Students will have the option of taking courses in both online and offline (traditional face to face) formats.

e) What is the maximum number of students who would be enrolled in an online course section?

Online courses in the HCE program would adhere to the University at Albany standard operating procedure of capping classes at 25 students.

Part A: Institution-wide Issues: Submit Part A only for the **first** Distance Education program proposed by your institution using this form. SUNY and the State Education Department will keep this in a master file so that your institution will not need to resubmit it for each new proposed online program, **unless there are significant changes, such as a new platform.**

I.   ORGANIZATIONAL COMMITMENT

a) Describe your institution's planning process for Distance Education, including how the need for distance access was identified, the nature and size of the intended audiences, and the provisions for serving those audiences, including how each student's identity will be verified.

b) Describe your institution's resources for distance learning programs and its student and technical support services to ensure their effectiveness. What course management system does your institution use?

c) Describe how the institution trains faculty and supports them in developing and teaching online courses, including the pedagogical and communication strategies to function effectively. Describe the qualifications of those who train and/or assist faculty, or are otherwise responsible for online education.

d) If your institution uses courses or academic support services from ***another provider***, describe the process used (with faculty participation) to evaluate their quality, academic rigor, and suitability for the award of college credit and a degree or certificate.

e) Does your institution have a clear ***policy on ownership of course materials*** developed for its distance education courses? How is this policy shared with faculty and staff? ***NOTE:*** *You may refer to SUNY's statement on copyright and faculty ownership of instructional content, and/or faculty contract provisions.*

II.   LEARNER SUPPORT

a)   Describe how your institution provides distance students with *clear information* on:
- Program completion requirements
- The nature of the learning experience
- Any specific student background, knowledge, or technical skills needed
- Expectations of student participation and learning
- The nature of interactions among faculty and students in the courses.
- Any technical equipment or software required or recommended.

b)   Describe how your institution provides distance learners with adequate *academic and administrative support*, including academic advisement, technical support, library and information services, and other student support services normally available on campus. Do program materials clearly define how students can access these support services?

c)   Describe how *administrative processes* such as admissions and registration are made available to distance students, and how program materials inform students how to access these services.

d)   What *orientation* opportunities and resources are available for students of distance learning?

Part B: Program-Specific Issues: Submit Part B for each new request to add Distance Education Format to a proposed or registered program.

III.   LEARNING DESIGN

a)   How does your institution ensure that the *same academic standards and requirements* are applied to the program on campus and through distance learning? If the curriculum in the Distance Education program differs from that of the on-ground program, please identify the differences.

Both the online and on campus programs were constructed by the same faculty group, which is comprised of primarily tenured and tenure-track faculty with input from highly experienced Public Service Professors (professors that are professionally rather than academically qualified to teach in the program. For instance, our faculty group includes a 33-year CIA veteran with a PhD and a former brigadier general with teaching experience at West Point.) The program will not be principally staffed by temporary faculty. Advising for all certificate students, whether online or on campus, will be handled by members of the faculty group.

With two exceptions, all courses offered online are offered on campus using the same syllabus with some modifications for online purposes (for instance, using online small groups rather than in-class small group discussions). The core cybersecurity and emergency management courses, PAD 545 and PAD 555, were developed from origin as online courses (in-class courses based on the existing syllabus will be developed during the 2015 calendar year). Courses are of the same length and have the same assignments and examinations.

b)   Are the courses that make up the distance learning program offered in a sequence or configuration that allows *timely completion of requirements*?

Yes. PAD 557, which is required of all students in the HCE program, will be taught both online and in a face-to-face format each academic year. In addition, the required course for each track (PAD 554, PAD 545 and PAD 555) will be offered online each academic year. Although all elective courses for each track will not be offered yearly, a sufficient number (at least 3) will be offered online each academic year to allow students to complete the certificate in one year. The sequence that the courses are offered each year will be carefully thought out to ensure that students have appropriate classes to choose from to complete the core and elective requirements.

c) How do faculty and others ensure that *the technological tools* used in the program are appropriate for the content and intended learning outcomes?

In the process of developing new courses, faculty members and staff will test technological tools in cooperation with the Course Management and Instructional Technology division of the University at Albany's Information Technology Services (ITS) and the UAlbany teaching and learning center (the Institute for Teaching, Learning and Academic Leadership, ITLAL). With the assistance of ITS and ITLAL, we will develop a standard training module for all public service professors, adjunct faculty and tenure track faculty using the technology for the first time. Rockefeller College has also received a distance learning grant from the UAlbany Provost's office that will support training of faculty and graduate students in synchronous and asynchronous distance learning. We anticipate that this grant will support fielding more elective courses in distance learning format, particularly in the HCE and proposed Master of International Affairs (MIA) programs.

d) How does the program provide for appropriate and flexible interaction between faculty and students, and among students?

Faculty members will be available to interact with students through a variety of means – in person during office hours or scheduled appointments, via telephone, and/or via the use of Adobe Connect (or similar software) or Skype for students who prefer face to face interaction but are unable to meet in person due to distance or some other limitation. The technology that will be used for the classes will also allow interaction between students and faculty and students and students through message boards and file sharing systems.

e) How do faculty teaching online courses verify that the student who registers in a distance education course or program is the same student who participates in and completes the course or program and receives the academic credit?

Faculty members will be required to abide by the University at Albany's ITS policy on identity access and management (available at https://wiki.albany.edu/display/public/askit/Identity+Access+ and+Management+Policy). These policies ensure that the student who registers in a distance education program is the same student who participates in and completes the program and thus receives the academic credit. UAlbany students who participate in such classes are required to use secure login procedures for their online classes. Every student will be required to use the unique online identity (PIN, Albany ID, NetID) that is assigned to them by the University. A password is established by the student for the purpose of authenticating their assigned identity. PINS and passwords are confidential and must not be shared with anyone.

IV. OUTCOMES AND ASSESSMENT

a) Distance learning programs are expected to produce the **same learning outcomes** as comparable classroom-based programs. How are these learning outcomes identified – in terms of knowledge, skills, or credentials – in course and program materials?

Distance learning courses will have learning objectives stated in course syllabi. The learning outcomes for these courses will be the same as equivalent courses taught in the traditional face to face classroom setting.   These learning outcomes will be assessed according to the schedule provided in Form 2C and outlined in section V below.

b) Describe how the **means chosen for assessing student learning** in this program are appropriate to the content, learning design, technologies, and characteristics of the learners.

Courses will use examinations, written assignments, homework problem sets, group projects, and class participation as means of assessing student learning. These methods are commonly used throughout the College's other comparable programs.

V. PROGRAM EVALUATION

a) What process is in place to monitor and **evaluate the effectiveness** of this particular distance education program on a regular basis?

The distance education courses offered as part of the HCE program will be evaluated according to the same standards used to evaluate and asses all courses, including traditional classroom courses. The learning objectives of the core courses will be assessed on a bi-annual basis for the first two-years after the program is initiated by the homeland security program director. One core course per semester will be assessed to determine if student learning outcomes are being met. After this initial assessment cycle, courses will be reviewed on an annual basis (courses will be assessed in the same order as they were initially assessed). After each course assessment, the homeland security program chair will determine if additional assessment of the core courses is needed. Additional assessment would be required if it was determined during the initial assessment that the learning objectives were not being met and if changes to the course were recommended. If it is determined that an additional assessment is needed, this would take place the following semester in which the class was taught. If it is determined that no additional assessments are immediately needed, the annual assessment of each core course (one per year) will be continued according to schedule. Once the core courses have all be assessed positively, elective courses will be assessed (one per year).

b) How will the evaluation results be used for **continuous program improvement**?
If it is determined that learning objectives are not being met in any of the HCE program courses, the program director would meet with all faculty responsible for teaching the course to determine how the content and delivery of the course material could be improved so that learning objectives are met. This would include comparison of course content to comparable courses both within the University at Albany and at similar programs in peer institutions. Should it be determined that the delivery of the material is not meeting expectations, faculty members would be required to seek training from the Course

6

Management and Instructional Technology division of the University at Albany's Information Technology Services (ITS) and the UAlbany teaching and learning center (the Institute for Teaching, Learning and Academic Leadership, ITLAL).

c) How will the evaluation process assure that the ***program results in learning outcomes appropriate to the rigor and breadth*** of the college degree or certificate awarded?

The director of the HCE program, in consultation with the dean of Rockefeller College, will review learning outcomes in conjunction with graduation statistics, average time-to-degree and student career placements (e.g., percent placed, average wage, field of specialization) compiled annually by the director of internships and career services. Emergency Preparedness, Homeland Security, and Cybersecurity alumni will also be regularly surveyed to determine career trajectories and how our programs could be altered to better equip our students for a competitive job environment.

VI. STUDENTS RESIDING OUTSIDE NEW YORK STATE

SUNY programs must comply with all "authorization to operate" regulations that are in place in other U.S. states where the institution has enrolled students or is otherwise active, based on each state's definitions.

a) What processes are in place to monitor the U.S. state of residency of students enrolled in any distance education course in this program while residing in their home state?

The University at Albany Graduate Admissions Office and the Office of the Registrar monitor and verify residency for all graduate students.

b) Federal regulations require institutions delivering courses by distance education to provide students or prospective students with contact information for filing complaints with the state approval or licensing entity in the student's state of residency and any other relevant state official or agency that would appropriately handle a student's complaint. What is the URL on your institution's website where contact information for filing complaints for students in this program is posted? ***NOTE:*** *Links to information for other states can be found at* http://www.suny.edu/provost/dlo/dl_outofstate.cfm.

http://www.albany.edu/graduatebulletin/requirements_student_complaints.htm

Version 2013-10-15