THE GRADUATE SCHOOL - UNIVERSITY OF RHODE ISLAND
NEW PROGRAM REPORT FROM THE GRADUATE COUNCIL TO THE FACULTY SENATE
CURRICULAR REPORT #2014-15-8A; 26 January 2015

At Meeting No. 487 held on 26 January 2015, the Graduate Council approved the attached proposal that is now submitted to the Faculty Senate.

SECTION I
ABSTRACT AND BACKGROUND INFORMATION

ABSTRACT (modified from proposal)

The Graduate Council approved a proposal from the College of Arts and Sciences to create a ***Professional Science Masters Degree (PSM) in Cyber Security***. What is proposed is a completely online Professional Science Masters (PSM) in Cyber Security that is designed to provide students with the fundamental technical, legal, and procedural concepts required in Cyber Security, along with exposure to professional expertise in the field. Cyber Security is the discipline involved with preventing, detecting and responding to attacks on computer systems and networks. It includes Digital Forensics, which is the investigation of legal matters through digital evidence (emails, files, text messages, etc). The Cyber Security field requires an in-depth understanding of computer science and computer systems as well as social/legal issues, and business procedures.

BACKGROUND

A PSM degree is a nationally recognized designation (www.sciencemasters.com/) and one with significant national momentum, which differentiates a student over a typical MS student because the PSM includes a professional component that exposes students to business skills that are crucial to be a successful cyber security specialist within an organization. Upon completion of the program, the acquired technical skills along with the professional skills will make the student highly marketable in an already high demand field. The PSM in Cyber Security will have three core courses and two tracks from which to choose. The core will emphasize fundamental cyber security skills as well as professional skills, including an internship to provide hands-on, real-world practice with a partner organization. The two tracks will reflect the strengths that we have already established with our existing graduate certificate programs. The forensics track will allow students to focus on digital forensics skills, while the security track includes courses with a focus on systems and network security, penetration testing and intrusion detection.

SECTION II
RECOMMENDATION

The Graduate Council approved the proposal to create a ***Professional Science Masters Degree (PSM) in Cyber Security*** at its Meeting No. 487 held on 26 January 2015, and forwards it to the Faculty Senate with a recommendation for approval.

THE
UNIVERSITY
OF RHODE ISLAND

THINK BIG WE DO™

Academic Program Proposal Cover Page

1. Name/Contact Information: Lisa DiPippo

2. Originating from (please fill in all that apply):

Computer Science and Statistics	Arts and Sciences	
(Department)	(School/College)	(Division)

3. Program type: Undergraduate □ (attach Curriculum Sheet) Graduate ☑ (attach List of Requirements)

4. Proposing **New** ☑ or **Change** □ to the following (see **Instructions** for definitions): (select all that apply)

Department: □ Degree: ☑ Program: ☑ Major: □ Sub plan: □ (option, track, concentration) Other: □

Title/name of proposed Department:

Title/name of proposed Degree:

Title/name of proposed Program: Cyber Security Professional Science Master's

Title/name of proposed Major:

Classification of instruction program (CIP) code: CIP Index 11.1003

Title/name of proposed Sub plan:

CIP code (if different from above): CIP Index

Other:

5. Proposed Degree(s) (BS, BA, BFA, MA, MS, Ph.D, etc.): MS

6. Intended initiation date: Term Fall Year 2015

7. Anticipated date of granting first degree: May 2018

8. Intended location of program: Kingston ☑ Providence □ Narragansett Bay Campus □

9. Total Credits Required for Graduation: (120, 130, etc) 36

10. Certification/Licensing Requirements: Yes □ (provide brief description) No ☑

Office Use Only:
College Curriculum Committee __________ Curricular Affairs Committee __________ Graduate Council __________
Faculty Senate __________ President __________ RIBGHE __________ Enrollment Services __________

THE
UNIVERSITY
OF RHODE ISLAND
Full Proposal Form RIBGHE

Revised 10-2009

A Proposal for Cyber Security Professional Science Master's Degree
Date: October 20, 2014

A. PROGRAM INFORMATION

A1. Name of institution

University of Rhode Island

A2. Name of department, division, school or college

Department – Computer Science and Statistics
College – Arts and Sciences

A3. Title of proposed program and Classification of Instructional Programs (CIP) code

Program title – *Cyber Security Professional Science Master's Degree*
Classification code (CIP)

A4. Intended initiation date of program change. Include anticipated date for granting first degrees or certificates, if appropriate.

Initiation date – Fall 2015
First degree date – Spring 2017

A5. Intended location of the program

Kingston

A6. Description of institutional review and approval process

	Approval Date
Department	
College	
CAC/Graduate Council	
Faculty Senate	
President of the University	

A7. Summary description of proposed program (not to exceed 2 pages)

We are proposing a completely online Professional Science Masters (PSM) in Cyber Security that is designed to provide students with the fundamental technical, legal, and procedural concepts required in *Cyber Security*, along with exposure to professional expertise in the field. Cyber Security is the discipline involved with preventing, detecting and responding to attacks on computer systems and networks. It includes *Digital Forensics*, which is the investigation of legal matters through digital evidence (emails, files, text messages, etc). The Cyber Security field requires an in-

depth understanding of computer science and computer systems as well as social/legal issues, and business procedures.
A PSM degree, which is a nationally-recognized designation (www.sciencemasters.com/) and one with significant national momentum, will differentiate a student over a typical MS student because the PSM includes a professional component that exposes students to business skills that are crucial to be a successful cyber security specialist within an organization. Upon completion of the program, the acquired technical skills along with the professional skills will make the student highly marketable in an already high-demand field.

The market for cyber security jobs is large and continuing to grow. According to Burning Glass International Inc., a Boston-based company that uses artificial intelligence to match jobs and job seekers, cyber security postings have grown 74% from 2007 to 2013 – twice as fast as all IT jobs. The report also indicates that the demand for cyber security talent is exceeding the supply. These job postings took 36% longer to fill than all job postings. There is a dire need for professionals in the field to fill these positions.

Currently URI has an online Graduate Certificate in Cyber Security and an online Graduate Certificate in Digital Forensics. When these programs were initially conceived, there was high demand for this type of program, and they were relatively rare. Recently, more institutions have developed similar programs, as well as master's programs, indicating the need for URI to provide a more advanced degree to remain competitive in the market. While there are several existing master's programs in cyber security in New England, very few are completely online. Further, there is currently no existing PSM program in cyber security. During a talk with faculty at URI in Spring 2014, the Director of the University of North Carolina Systemwide PSM Program, highlighted cyber security as an area ripe for the development of a PSM. She encouraged URI to pursue this opportunity.

The PSM in Cyber Security will have three core courses and two tracks from which to choose. The core will emphasize fundamental cyber security skills as well as professional skills, including an internship to provide hands-on, real-world practice with a partner organization. The two tracks will reflect the strengths that we have already established with our existing graduate certificate programs. The forensics track will allow students to focus on digital forensics skills, while the security track includes courses with a focus on systems and network security, penetration testing and intrusion detection.

The existing graduate certificates in cyber security and digital forensics are run through URI's College of Continuing Education Special Programs, making them self-sustaining. In proposing this PSM in Cyber Security, we plan to continue to utilize this successful mechanism. With the graduate certificate programs as feeders, we do not anticipate requiring any additional resources to start-up the PSM in Cyber Security. We are adding two new courses, CSF 580 – Professional Skills for Cyber Security, and CSF 590 – Cyber Security Internship, both of which will be required for all students in the program.

Cyber Security PSM Requirements:

The degree will require 36 credits, which will consist of 9 4-credit courses. There will be no Comprehensive Exam and no thesis requirement. However, CSF 590 will provide a capstone experience through an internship with a partner organization.

Students will be required to take four core courses, and choose from one of two tracks, a Forensics Track and a Security Track.

Core Courses
1) CSF 430 (Introduction to Information Assurance)
2) CSF 432 (Introduction to Network and Systems Security)
3) CSF 580 (Professional Skills for Cyber Security)
4) CSF 590 (Cyber Security Internship)

Forensics Track
5) CSF 410 (Digital Forensics 1)
6) CSF 512 (Digital Forensics 2)
7) CSF 414 (Digital Forensics Analysis)
8) CSF 516 (File Systems Analysis)
9) CSF 524 (Advanced Incident Response)

Security Track
5) CSF 534 (Advanced Network and Systems Security 2)
6) CSF 410 (Digital Forensics 1)
7) CSF 524 (Advanced Incident Response)
8) CSF 538 (Penetration Testing)
9) CSF 536 (Advanced Intrusion Detection and Defense) or CSF 512 (Digital Forensics 2)

A8. Signature of the President

____
David M. Dooley

A9. Person to contact during the proposal review

Name: Lisa DiPippo
Title: Professor
Phone: 874-2701
Email: dipippo@cs.uri.edu

A10. Signed agreements for any cooperative arrangements made with other institutions/agencies or private companies in support of the program.

B. RATIONALE: There should be a demonstrable need for the program

B1.State the program objectives.

The objectives of the Professional Science Master's Degree in Cyber Security are to ensure that upon completion of the program, students will be able to:

- Identify threats to the critical information assets of an organization.
- Characterize privacy, legal and ethical issues of information security.
- Manage, control and mitigate risk to critical information assets.
- Identify vulnerabilities in an organization's computer systems and networks.
- Define the security controls sufficient to provide a required level of confidentiality, integrity, and availability in an organization's computer systems and networks.
- Diagnose attacks on an organizations computer systems and networks and propose solutions including development, modification and execution of incident response plans.
- Apply critical thinking and problem-solving skills to address current and future attacks on an organization's computer systems and networks.
- Communicate, orally and in writing, proposed information security solutions to technical and non-technical decision-makers in an organization.
- Apply business principles to analyze and interpret data for planning, decision making, and problem solving in an information security environment.
- Motivate and organize collaborative teams and facilitate group work in an information security environment.

B2. Explain and quantify the needs addressed by this program, and present evidence that the program fulfills these needs.

The market for cyber security jobs is large and continuing to grow. According to Burning Glass International Inc., a Boston-based company that uses artificial intelligence to match jobs and job seekers, cyber security postings have grown 74% from 2007 to 2013 – twice as fast as all IT jobs. The report also indicates that the demand for cyber security talent is exceeding the supply. These job postings took 36% longer to fill than all job postings. There is a dire need for professionals in the field to fill these positions.

Students completing the Cyber Security PSM will be well-equipped to fill the jobs that are described above. The program will instill strong skills in specific technical areas. In addition, they will acquire the professional skills necessary to work in a variety of industries and government agencies with a critical need for cyber security experts.

B3. If an external advisory or steering committee was used to develop the program, identify committee members and their affiliations and describe the committee's role.

Not applicable.

C. INSTITUTIONAL ROLE: The program should be clearly related to the published role and mission of the institution and be compatible with other programs and activities of the institution.

C1. Explain how the program is consistent with the published role and mission of the institution and how it is related to the institution's academic planning.

The proposed online PSM in Cyber Security connects with the mission of the University by offering an innovative, online program to students in Rhode Island and beyond. It addresses several aspects of the Academic Plan, in particular:

Goal I: Enhance Academic Quality and Value – Expanding online offerings; Majors with a high proportion of the curriculum provided online.

The PSM in Cyber Security will be a fully online masters degree. The success of the existing online graduate certificates in cyber security and digital forensics provides evidence that we can create effective online courses and implement a successful online program.

Goal II: Prepare Students for a Changing World – Boost experiential learning for undergraduate and graduate students.

The online PSM in Cyber Security has professional experience at its core. We will partner with various organizations that will serve as advisors and mentors to students in their required internships.

C2. Explain the relationship of the program to other programs offered by the institution.

The Cyber Security PSM will be offered through the Department of Computer Science and Statistics. The department offers several related programs.

Master's Degree in Computer Science

The Master's Degree in Computer Science will have a slight overlap with the Cyber Security PSM in that some of the same courses will be accepted in both programs. The Computer Science MS allows students to take CSF courses if they are related to the research that the student has undertaken. There are two main differences between these two programs:

1) The Computer Science MS requires a substantial computer science background, most often a BS in Computer Science or a related field. On the other hand, the Cyber Security PSM requires no prior computer science knowledge. The prerequisite knowledge for the Cyber Security PSM is

related more to information technology, and can be acquired either from prior educational / professional experience, or through a set of online modules that we will make available to students prior to taking the first course in the program.

2) The Computer Science MS has a research component. Students in this program are required to either do a thesis, or take a comprehensive exam. In the Cyber Security PSM, there is no thesis or comprehensive exam. Instead, the students will be required to take a capstone course that will allow them to demonstrate their overall knowledge of the track they have chosen.

We anticipate that very few students who would apply to the MS in Computer Science will instead apply to the Cyber Security PSM because the backgrounds that are required are different and because the content of the programs are significantly different.

Graduate Certificates in Cyber Security and in Digital Forensics
The Department of Computer Science and Statistics also offers Graduate Certificates in Cyber Security and in Digital Forensics. These programs are closely related to the Cyber Security PSM. Each of the certificate programs requires four 4-credit courses. The Forensics Track of the Cyber Security PSM consists of five courses, three of which are required for the Digital Forensics Graduate Certificate, and the other two are optional for the certificate. Similarly, the Security Track for the Cyber Security PSM includes five courses, one of which is required for the Cyber Security Graduate Certificate, and the others are optional in the certificate program.

We anticipate that some of the students who would apply to the certificate programs will choose instead to enroll in the PSM. Other students will likely begin in one of the certificate programs and then migrate to the PSM. The courses that are taken towards the certificates will automatically apply towards the PSM if a student chooses to apply to the PSM after starting in a certificate program.

D. INTERINSTITUTIONAL CONSIDERATIONS: The program should be consistent with all policies of the Board of Governors pertaining to the coordination and collaboration between public institutions of higher education. (Consult the Board of Governors' *Coordination Plan for Academic Programs in Rhode Island Public Institutions of Higher Education* [www.ribghe.org/publicreg.htm] for guidelines and restrictions regarding the types and levels of programs the institutions are allowed to offer.)

D1. List similar programs offered in the state and region, and compare the objectives of similar programs.

There are no similar programs offered by any of the other public institutions in Rhode Island. Of the private institutions in RI, none offers a Professional Science Master's Degree in Cyber Security.

Salve Regina University offers a Certificate of Graduate Studies in Cybersecurity and Intelligence. This is a 12 credit certificate covering non-technical aspects of cyber security including intelligence and policy management.

Roger Williams University offers a Master of Science in Cybersecurity. This program has similar course requirements to the proposed Cyber Security PSM. However, it does not have the professional component to it. Further, it is not offered online as the proposed program is.

Brown University offers a ScM Degree in Computer Science that is similar to the Computer Science MS at URI. This program is not comparable to the proposed Cyber Security PSM for the same reasons that the URI Computer Science MS is different.

D2. Estimate the projected impact of program on other public higher education institutions in Rhode Island (e.g. loss of students or revenues), provide a rationale for the assumptions made in the projections, and indicate the manner in which the other public institutions were consulted in developing the projections.

The proposed Cyber Security PSM will have no impact on other public higher education institutions in RI because none of them offers graduate programs in this field.

D3. Using the format prescribed by RIOHE, describe provisions for transfer students (into or out of the program) at other Rhode Island public institutions of higher education. Describe any transfer agreements with independent institutions. The institution must also either submit a Joint Admissions Agreement transition plan or the reason(s) the new program is not transferable. (See *Procedure for Strengthening the Articulation/Transfer Component of the Review Process for New Programs* which can be found at *www.ribghe.org/publicreg.htm*.)

We do not expect any transfer students into our program for other RI public institutions because it is a graduate program in an area not addressed by the other institutions.

D4. Describe any cooperative arrangements with institutions offering similar programs. (Signed copies of any agreements pertaining to use of faculty, library, equipment, and facilities should be attached.)

Not applicable.

D5. If external affiliations are required, identify providing agencies (Indicate the status of any arrangements made and append letters of agreement, if appropriate.)

Not applicable.

D6. Indicate whether the program will be available to students under the New England Board of Higher Education's (NEBHE) Regional Student Program (RSP).

Not applicable.

E. PROGRAM: The program should meet a recognized educational need and be delivered in an appropriate mode.

E1. Prepare a typical curriculum display for one program cycle for each sub-major, specialty or option, including the following information:

a. **Name of courses, departments, and catalog numbers and brief descriptions for new courses, preferably as these will appear in the catalog. In keeping with each institution's timetable for completion of student outcomes assessment, each institution should provide an assessment plan detailing what a student should know and be able to do at of the program and how the skills and knowledge will be assessed. For example, if a department brings forth a new program proposal but that department is not slated to have its student outcomes assessment completed until 2008, the program could be approved but with the provision that the department return no later than 2008 and present to the Academic and Student Affairs Committee its student outcomes for that particular program.**

Department:

All of the courses will be offered through the Digital Forensics and Cyber Security Center within the Department of Computer Science and Statistics. The courses will all be delivered online.

Cyber Security PSM Requirements:

The degree will require 36 credits, which will consist of 9 4-credit courses. There will be no Comprehensive Exam and no thesis requirement. However, CSF 590 will provide a capstone experience through an internship with a partner organization.

Students will be required to take four core courses, and choose from one of two tracks, a *Forensics Track* and a *Security Track*.

(New courses are identified by * with full catalog descriptions found below)

<u>Core Courses</u>

1) CSF 430 (Introduction to Information Assurance)
2) CSF 432 (Introduction to Network and Systems Security)
3) CSF 580 (Professional Skills for Cyber Security)*
4) CSF 590 (Cyber Security Internship)*

<u>Forensics Track</u>

5) CSF 410 (Digital Forensics 1)
6) CSF 512 (Digital Forensics 2)
7) CSF 414 (Digital Forensics Analysis)
8) CSF 516 (File Systems Analysis)

9) CSF 524 (Advanced Incident Response)

Security Track
5) CSF 534 (Advanced Network and Systems Security 2)
6) CSF 410 (Digital Forensics 1)
7) CSF 524 (Advanced Incident Response)
8) CSF 538 (Penetration Testing)
9) CSF 536 (Advanced Intrusion Detection and Defense) or CSF 512 (Digital Forensics 2)

Course Description:
CSF 580 – Professional Skills for Cyber Security
See attached syllabus. Course proposal is being submitted concurrent with this program proposal.
CSF 590 – Cyber Security Internship
See attached syllabus. Course proposal is being submitted concurrent with this program proposal.

Assessment Plan:

See Appendix B.

b. Required courses in area of specialization and options, if any

There are two tracks in the proposed program: *Forensics* and *Security*. Each track requires that a student take the 4 required courses and then take 5 courses in the chosen track. The tracks are as follows:

Forensics Track
CSF 410 (Digital Forensics 1)
CSF 512 (Digital Forensics 2)
CSF 414 (Digital Forensics Analysis)
CSF 516 (File Systems Analysis)
CSF 524 (Advanced Incident Response)

Security Track
CSF 534 (Advanced Network and Systems Security 2)
CSF 410 (Digital Forensics 1)
CSF 524 (Advanced Incident Response)
CSF 538 (Penetration Testing)
CSF 536 (Advanced Intrusion Detection and Defense) or CSF 512 (Digital Forensics 2)

c. Course distribution requirements, if any, within program, and general education requirements

Not applicable.

d. Total number of free electives available after specialization and general education requirements are satisfied

None.

e. Total number of credits required for completion of program or for graduation. Present evidence that the program is of appropriate length as illustrated by conformity with appropriate accrediting agency standards, applicable industry standards, or other credible measure, and comparability of lengths with similar programs in the state or region.

The total number of credits required is 36. In a survey of existing Professional Science Master's programs in areas comparable to Cyber Security, the average number of credits was 36. The table below lists the existing PSM programs in related areas along with their credit requirements.

School	Degree	Credits
NC State	PSM Computer Networking	31
Rutgers	PSM Info Tech	43
UNC Wilmington	PSM CS and Info Sys	36
UMUC	PSM Information Assurance	39
UMUC	MS Cyber Security	36
Valparaiso	PSM Info Tech	33
College of Saint Rose	PSM CIS	33
	Average Credit Requirement	36

Find more information about PSM programs here: http://www.sciencemasters.com/.

f. Identify any courses that will be delivered or received by way of distance learning. (Refer to *www.ribghe.org/publicreg.htm* for the *Standards for Distance Learning in the Rhode Island System of Public Higher Education*.)

All courses offered in this program will be online.

E2. Describe certification/licensing requirements, if any, for program graduates and the degree to which completion of the required course work meets said requirements. Indicate the agencies and timetables for graduates to meet those requirements.

Not applicable.

E3. Include the learning goals (what students are expected to gain, achieve, know, or demonstrate by completion of the program) and requirements for each program.

The expected learning outcomes for the PSM in Cyber Security are as follows.

Upon completion of the Professional Science Master's in Cyber Security, a student will be able to:

- Identify threats to the critical information assets of an organization.
- Characterize privacy, legal and ethical issues of information security.
- Manage, control and mitigate risk to critical information assets.
- Identify vulnerabilities in an organization's computer systems and networks.
- Define the security controls sufficient to provide a required level of confidentiality, integrity, and availability in an organization's computer systems and networks.
- Diagnose attacks on an organizations computer systems and networks and propose solutions including development, modification and execution of incident response plans.
- Apply critical thinking and problem-solving skills to address current and future attacks on an organization's computer systems and networks.
- Communicate, orally and in writing, proposed information security solutions to technical and non-technical decision-makers in an organization.
- Apply business principles to analyze and interpret data for planning, decision making, and problem solving in an information security environment.
- Motivate and organize collaborative teams and facilitate group work in an information security environment.

E4. Demonstrate that student learning is assessed based on clear statements of learning outcomes and expectations.

a. Include the learning goals (what students are expected to gain, achieve, know, or demonstrate by completion of the program) requirements for each program

See E3 above.

b. Demonstrate that student learning is assessed based on clear statements of learning outcomes and expectations.

In Appendix B, we describe the preliminary assessment plan for the PSM in Cyber Security. This plan indicates how student learning will be assessed based on the learning outcomes listed above.

F. FACULTY AND STAFF: The faculty and support staff for the program should be sufficient in number and demonstrate the knowledge, skills, and other attributes necessary to the success of the program

F1. Describe the faculty who will be assigned to the program. Indicate total full-time equivalent (FTE) positions required for the program, the proportion of program faculty who will be in tenure-track positions, and whether faculty positions will be new positions or reassignment of existing positions.

The faculty assigned to the program will consist of one lecturer teaching 7-8 courses per year, and part-time faculty teaching 7-8 courses each year. The full-time lecturer will be a new position that will eventually be supported by the revenue generated by the program, but will initially (the first two years) require start-up support. See Appendix A for details.

Calculation of FTE positions: The program requires the instruction of 14 courses. A typical instructor's load is 8 courses. Since one may be a double course, we list his/her teaching load at 7-8 courses per year. The remaining courses will be taught by part-time instructors. One full-time instructor is essential for the consistency of the program. See Appendix A for details.

F2. List anticipated support staff, the percent of their time to be spent in the program, and whether these are reassignments or new positions. Indicate total full-time equivalent (FTE) positions required for the program.

The program will require hiring a program manager with full time devoted to administering the PSM program and managing relationships with external industry partners. The funds for this position will come from the revenue generated (See Budget and Budget Narrative documents in Appendix A).

F3. Summarize the annual costs for faculty and support staff by indicating salaries and fringe benefits (adjusted for the proportion of time devoted to the program). Distinguish between existing resources and new resources. Specify in the narrative if resources are to be provided by more than one department. (Include the salary and benefits information on the budget form that can be found at *www.ribghe.org/publicreg.htm*.)

See attached Budget and Budget Narrative documents in Appendix A.

F4. Provide assurance that the institution's chief academic officer has worked with the director of human resources (or equivalent) in the development of the faculty and staff projections and estimates and that they agree on the adequacy of the estimates.

The JCAP Committee has reviewed this proposal and has recommended that it go forward in its approval process.

G. STUDENTS: The program should be designed to provide students with a course of study that will contribute to their intellectual, social and economic well-being. Students selected should have the necessary potential and commitment to complete the program successfully.

G1. Describe the potential students for the program and the primary source of students. Indicate the extent to which the program will attract new students or will draw students from existing programs and provide a specific rationale for these assumptions. For

graduate programs, indicate which undergraduate programs would be a potential source of students.

The students for this program will come from several groups. There will be some professionals looking to further their cyber security education. There will be some people looking to change careers who may have limited to no prior cyber security background. And there will be some students directly after completing their undergraduate degrees looking to advance their cyber security knowledge and skills. We expect that the programs that will be impacted most by the addition of the PSM in Cyber Security will be the Graduate Certificate programs in Cyber Security and Digital Forensics. Many of the students who are currently enrolled in these programs have indicated their strong interest in completing a Master's degree in Cyber Security. Other potential students have told us that they would not be able to enroll in the certificate programs because their employers would not pay for them, but they would pay for a master's level program. We still expect some students to prefer the 4-course certificates for their quick time to completion. However, even after these students complete the requirements for the certificates, they will be allowed to transfer all of the credits earned if they decide to apply to the PSM later.

We do not anticipate that the addition of the PSM in Cyber Security will have much impact on the Master's in Computer Science for several reasons. First, the MS in Computer Science is a degree that requires a strong computer science background, typically a BS in Computer Science or a related field. The PSM in Cyber Security does not require such a background, although students with a BS in Computer Science may choose the PSM. Second, the MS in Computer Science usually includes a research component, whereas the PSM does not. While the MS in Computer Science does have a track for students interested in cyber security or digital forensics, these students are generally interested in doing research in these areas, and so would not generally choose the PSM.

The undergraduate programs that would be a potential source of students for the PSM in Cyber Security would include Computer Science, both BA and BS, Math, Computer Engineering, Business, Criminal Justice, etc. In fact, because the PSM does not require any specific background to apply, any undergraduate major is a potential source of students.

G2. Estimate the proposed program size and provide projected annual full-time, part-time, and FTE enrollments for one complete cycle of the program. Provide a specific rationale for the assumptions made in the projections. (Depending on the nature of the program, use the FTE or part-time estimates of enrollment on the budget form, which can be found at *www.ribghe.org/publicreg.htm*.)

See Budget and Budget Narrative documents in Appendix A.

G3. Indicate how the institution provides programs and services designed to assist students in achieving their academic goals.

The Program Manager position that we will create for this program will provide academic advising for students in the program. This will include help with the application process, answering questions about the academic requirements, and help with registering and choosing classes. The

Graduate School will provide the mechanisms for application and admission, as well as for monitoring progress towards graduation. We will work with the Center for Career and Experiential Education to build our internship program for the PSM in Cyber Security. The Program Manager and the instructor hired for this program will provide support to students in finding and working in their required internships.

G4. List the program admission and retention requirements for students. Provide descriptions of the specific criteria and methods used to assess students' ability to benefit from the program. Describe how satisfactory academic progress will be determined.

Admission will be determined based on performance in undergraduate program, and letters of recommendation provided. While we do not have a specified undergraduate GPA requirement, we will consider the whole application as a measure of potential success in the program for admission. In particular, we will look for applicants who demonstrate potential in technical fields, in problem solving and in working in teams. Once admitted, students' progress will be determined by satisfactory grades in the required courses as defined by the Graduate School, and good reports from mentors at their assigned internships.

G5. Indicate available funds for assistantships, scholarships and fellowships. (Include this information on the budget form, which can be found at *www.ribghe.org/publicreg.htm*.)

See Budget and Budget Narrative in Appendix A

H. ADMINISTRATION: Administrative oversight for the program should be sufficient to ensure quality.

H1. Indicate how the program will be administered and the degree to which this work will affect the administrative structure in which it is located.

The PSM in Cyber Security will be administered largely by the Program Manager described in the Budget and Budget Narrative in Appendix A. The Program Manager will work with the administrative in URI's Continuing Education Special Program's office and staff in the Computer Science and Statistics department to process applications through the Graduate School.

H2. Indicate the titles of the persons who will have administrative responsibility for the program and the percent of time each will spend on the program.

The Program Manager for the PSM in Cyber Security will have the majority of the administrative responsibility for the program. This manager will spend 100% of his/her time in this task. The secretary of the Computer Science and Statistics department will spend approximately 10% of her time working with the Program Manager on this administrative work.

H3. Indicate additional annual administrative salaries and related costs to be associated with the program. Distinguish between existing resources and new resources. (Include this information on the budget form, which can be found at *www.ribghe.org/publicreg.htm*.)

See Budget and Budget Narrative in Appendix A.

I. INSTRUCTIONAL RESOURCES: The instructional resources should be sufficient in quantity, quality and timeliness to support a successful program.

I1. Estimate the number and cost of relevant print electronic and other non-print library materials needed (and those available) for the program and compare with recommendations of national accrediting agencies, the standards of the Association of College and Research Libraries, and/or any other recognized measures of general library adequacy in terms of collections, staff, space and operations.

The added cost of print, electronic and other non-print library materials will be minimal for the PSM in Cyber Security. Any required journals, publications or subscriptions are already available through existing programs such as Computer Science MS, Graduate Certificates in Cyber Security and Digital Forensics.

I2. Identify and evaluate other instructional resources and instructional support equipment (such as computers, laboratory equipment and supplies) in terms of overall capability to satisfy the needs of the program. If these instructional resources are considered insufficient or if upgrading is necessary for the development of the program, the additional needs should be detailed and their cost estimated.

No additional instructional resources and instruction support equipment will be required for this program. The resources of the Digital Forensics and Cyber Security Center and the Department of Computer Science and Statistics are sufficient to run this proposed PSM in Cyber Security.

I3. Estimate annual expenditures for instructional resources. Distinguish between existing resources and new resources. The information should reflect the annual operation and maintenance of the instructional resources, recurrent costs and costs for necessary additions. (Include this information on the budget form, which can be found at *www.ribghe.org/publicreg.htm*.)

See Budget and Budget Narrative in Appendix A.

I4. Provide assurance that the institution's chief academic officer has worked with appropriate library and other staff in the development of the assessments and estimates regarding instructional resources and they are in agreement on the adequacy of estimates.

Library Impact Statement is attached.

J. FACILITIES AND CAPITAL EQUIPMENT: Facilities and capital equipment should be

sufficient in quantity, quality and timeliness to support a successful program.

J1. Describe the facilities and capital equipment (e.g., classrooms, office space, laboratories, and telecommunications equipment) and assess the adequacy of these resources relative to the program and to the requirements of the American with Disabilities Act and state disability statues.

The PSM in Cyber Security is a fully online program, so no facilities are required for the program. With respect to the ADA requirements, our online classes are designed using universal design principles and we work with the Office of Disability Services to make appropriate accommodations in these courses.

J2. If new or renovated facilities are necessary, explain in detail (e.g., requirements, costs, sources of revenue, and expected date of completion). (Include this information on the budget form, which can be found at *www.ribghe.org/publicreg.htm*.) [Note: the RIBGHE's Facilities Committee is responsible for approving lease, purchase or other agreements and ensuring that the facility meets all building, fire and health codes and ADA requirements.]

No additional facilities are required for the proposed PSM in Cyber Security.

J3. Estimate the annual additional expenditures for new program facilities and capital equipment. (Include this information on the budget form, which can be found at *www.ribghe.org/publicreg.htm*.)

Not applicable.

J4. Indicate whether the needed facilities are included in the institution's master plan.

Not applicable.

J5. Provide assurance that the institution's chief academic officer has worked with the facilities director (or equivalent) in the development of assessments and estimates regarding facilities and capital equipment and that they agree on the adequacy of estimates.

No applicable.

K. FINANCIAL CONSIDERATIONS: Projected revenues should be sufficient to support a successful program and must cover the estimated costs of the program.

K1. Expenditures for program initiation and annual operation should be estimated and displayed in the proposed budget. The summary should enable the reader to understand expenditures for a period representative of one full program cycle.

See Budget and Budget Narrative in Appendix A.

K2. Revenue estimates should be provided for a similar period of time. For a new program, the appropriateness and feasibility of instituting differential tuition and/or fees should be addressed.

NOTE: **Excel budget forms, which are self-calculating, may be downloaded from the RIOHE website at *www.ribghe.org/publicreg.htm*. Contact RIOHE's Academic and Student Affairs division for assistance in completing the forms.**

See Budget and Budget Narrative in Appendix A.

K3. Describe how current institutional resources will be redeployed or extra institutional resources will be obtained to support the program (e.g., describe program eliminations, staff reallocations and/or external sources of monies).

See Budget and Budget Narrative in Appendix A.

K4. Provide assurance that the institution's chief academic officer has worked with budget director and controller in the development of the financial projections and that they agree on the adequacy of the estimates.

The Office of Budget and Financial Planning has reviewed the budget and the response letter is included in Appendix A.

L. EVALUATION: Appropriate criteria for evaluating the success of a program should be development and used.

L1. List the performance measures by which the institution plans to evaluate the program. Indicate the frequency of measurement and the personnel responsible for performance measurements. Describe provisions made for external evaluation, as appropriate.

The following measures will be used to evaluate the program. All evaluations will be performed annually.

1. Enrollment of Students – new students in the program each year as well as retention of students throughout the program will be measured.
2. Course Evaluations – student evaluations of instructors will be performed each semester.
3. Program Evaluation by Advisory Board – Surveys of members of the advisory board will be taken each year with evaluation of current courses, and student performance in internships.

L2. Describe and quantify the program's criteria for success.

The following criteria will be used for success:

1. Enrollment of Students – 10, 15, 20, 25 students in years 1-4.
2. Course Evaluations – Overall ratings of each course will be at least 3 (on a scale of 1-5).
3. Program Evaluation by Advisory Board – Overall rating on the quality of the program, and on the performance of students will be at least 3 (on a scale of 1-5).

L3. If the proposed program is eligible for specialized accreditation, indicate name and address of the accrediting agency and a list of accreditation requirements. If specialized accreditation is available but not sought, indicate reasons.

Not applicable.

L4. Describe the process that communicates the results of the program evaluation to appropriate institutional stakeholders and uses the outcomes for program improvement.

The results of the evaluation will be communicated to the relevant parties each year, and the data will be used to improve the program. The relevant parties at URI include the faculty of the Department of Computer Science and Statistics, the Dean of the Graduate School, and the Office of the Provost. The Director of the Digital Forensics and Cyber Security Center will meet with instructors and course managers to review the results of the evaluations and plan for improvements in the program.

Response to the specific recommendations that came from the JCAP committee for the A&S Curriculum Committee.

Here is a brief response:

1) Consider adding a capstone/comprehensive exam requirement

Response: Following the JCAP meeting, we modified our program requirements to add another course that addresses business components of cyber security. This course will have a capstone project involved. Further, there is an internship requirement for the program. This will be a supervised internship with an associated course that students will attend and share experiences with each other. This course is the capstone experience for the PSM program.

2) Contact Experiential Learning Office and Career Development to confer about internships and to develop online professional skills seminar program

We have plans to contact the Experiential Learning Office before the internship course runs. This course will not run in the first year of the program because students will not be prepared and will be taking the earlier classes.

3) Consider establishing an external advisory committee

We are working with Joan Peckham to establish an advisory committee for the Computer Science and the Cyber Security / Digital Forensics programs. We have a preliminary list and are in the process of setting up initial meetings. This committee will be integral to our program because the members will likely be involved in providing internship opportunities to our students. They will also provide guidance on the continuous modification to the curriculum and courses.

4) Work with the Office of Research and Development on policy and controls for accepting international students

We have begun discussions with Gerry Sonnenfeld in the Office of Research and Development to understand the policies involved with accepting international students.

Please let me know if you have any questions about this. We look forward to discussing the proposal at the A&S Curriculum Committee meeting on Wed.

Thanks,

Lisa DiPippo

THE
UNIVERSITY
OF RHODE ISLAND

THINK BIG WE DO™

Joint Committee on Academic Planning Pre-Proposal for New Programs

Program Name: Professional Science Masters Degree in Cyber Security

Degree Type: Masters Degree

Proposer: Lisa DiPippo and Victor Fay-Wolfe

Department(s): Computer Science and Statistics

College(s): Arts and Sciences

Part 1. Briefly describe program.

We are proposing a completely online Professional Science Masters (PSM) in Cyber Security that is designed to provide students with the fundamental technical, legal, and procedural concepts required in *Cyber Security*, along with exposure to professional expertise in the field. Cyber Security is the discipline involved with preventing, detecting and responding to attacks on computer systems and networks. It includes *Digital Forensics*, which is the investigation of legal matters through digital evidence (emails, files, text messages, etc). The Cyber Security field requires an in-depth understanding of computer science and computer systems as well as social/legal issues, and business procedures.

A PSM degree, which is a nationally-recognized designation (www.sciencemasters.com/) and one with significant national momentum, will differentiate a student over a typical MS student because the PSM includes a professional component that exposes students to business skills that are crucial to be a successful cyber security specialist within an organization. Upon completion of the program, the acquired technical skills along with the professional skills will make the student highly marketable in an already high-demand field.

The market for cyber security jobs is large and continuing to grow. According to Burning Glass International Inc., a Boston-based company that uses artificial intelligence to match jobs and job seekers, cyber security postings have grown 74% from 2007 to 2013 – twice as fast as all IT jobs. The report also indicates that the demand for cyber security talent is exceeding the supply. These job postings took 36% longer to fill than all job postings. There is a dire need for professionals in the field to fill these positions.

Currently URI has an online Graduate Certificate in Cyber Security and an online Graduate Certificate in Digital Forensics. When these programs were initially conceived, there was high demand for this type of program, and they were relatively rare. Recently, more institutions have developed similar programs, as well as master's programs, indicating the need for URI to provide a more advanced degree to remain competitive in the market. While there are several existing master's programs in cyber security in New England, very few are completely online. Further, there is currently no existing PSM program in cyber security. During a talk with faculty at URI in Spring 2014, the Director of the University of North Carolina Systemwide PSM Program, highlighted cyber security as an area ripe for the development of a PSM. She encouraged URI to pursue this opportunity.

The PSM in Cyber Security will have three core courses and two tracks from which to choose. The core will emphasize fundamental cyber security skills as well as professional skills, including an internship to provide hands-on, real-world practice with a partner organization. The two tracks will reflect the strengths that we have already established with our existing graduate certificate programs. The forensics track will allow students to focus on digital forensics skills, while the security track includes courses with a focus on systems and network security, penetration testing and intrusion detection.

The existing graduate certificates in cyber security and digital forensics are run through URI's College of Continuing Education Special Programs, making them self-sustaining. In proposing this PSM in Cyber Security, we plan to continue to utilize this successful mechanism. With the graduate certificate programs as feeders, we do not anticipate requiring any additional resources to start-up the PSM in Cyber Security. We are adding only one new course, CSF 590 – Cyber Security Professional Skills, which will be required for all students in the program.

Part 2. How does the program connect to the mission of the University and the strategic themes and goals of the Academic Plan?

The proposed online PSM in Cyber Security connects with the mission of the University by offering an innovative, online program to students in Rhode Island and beyond. It addresses several aspects of the Academic Plan, in particular:

Goal I: Enhance Academic Quality and Value *– Expanding online offerings; Majors with a high proportion of the curriculum provided online.*

> The PSM in Cyber Security will be a fully online masters degree. The success of the existing online graduate certificates in cyber security and digital forensics provides evidence that we can create effective online courses and implement a successful online program.

Goal II: Prepare Students for a Changing World *– Boost experiential learning for undergraduate and graduate students.*

> The online PSM in Cyber Security has professional experience at its core. We will partner with various organizations that will serve as advisors and mentors to students in their required internships.

Part 3. Signatures

Proposer: Lisa DiPippo Digitally signed by Lisa DiPippo DN: cn=Lisa DiPippo, o=University of Rhode Island, ou=Department of Computer Science and Statistics, email=dipippo@cs.uri.edu, c=US Date: 2014.09.02 15:13:28 -05'00' Date: 9/1/2014

Chair(s): [illegible] Date:

Dean(s): Date: 9/4/2014

JCAP Review Committee Response: Date:

X We urge you to move the proposal forward for further development

____ We urge you to re-consider the proposed program

Comments:

You are urged to move the proposal forward for further development. Recommendations: 1) consider adding a capstone/comprehensive exam requirement; 2) contact the Experiential Learning Office and Career Development to confer about internships and to develop an online professional skills seminar for the program; 3) consider establishing an external advisory committee; 4) work with the Office of Research and Economic Development on policy and controls for accepting international students.

STANDARD ACADEMIC PROGRAM CHANGES
BUDGET FORM: Page 1 of 3

Use this form for programs that can be pursued on a full-time basis or through a combination of full-time and part-time attendance

REVENUE ESTIMATES

	Year 1 20__		Year 2 20__		Year 3 20__		Year 4 20__	
Full-Time Tuition Rate: In-State	**7500**		**7500**		**7500**		**7500**	
Full-Time Tuition Rate: Out-State	**7500**		**7500**		**7500**		**7500**	
Mandatory Fees per Student								
FTE # of New Students: In-State	**8**		**12**		**12**		**12**	
FTE # of New Students: Out-State	**8**		**12**		**12**		**12**	
# of In-State FTE Students transferring in from the institution's existing programs								
# of Out-State FTE Students transferring in from the institution's existing programs								
Tuition and Fees	Newly Generated Revenue	Revenue from existing programs	Newly Generated Revenue	Revenue from existing programs	Newly Generated Revenue	Revenue from existing programs	Newly Generated Revenue	Revenue from existing programs
First Year Students								
Tuition								
In-State	60,000	-	90,000	-	90,000	-	90,000	-
Out-of-State	60,000	-	90,000	-	90,000	-	90,000	-
Mandatory Fees	-	-	-	-	-	-	-	-
Second Year Students								
Tuition								
In-State			60,000	-	90,000	-	90,000	-
Out-of-State			60,000	-	90,000	-	90,000	-
Mandatory Fees			-	-	-	-	-	-
Third Year Students								
Tuition								
In-State					60,000	-	90,000	-
Out-of-State					60,000	-	90,000	-
Mandatory Fees					-	-	-	-
Fourth Year Students								
Tuition								
In-State							60,000	-
Out-of-State							60,000	-
Mandatory Fees							-	-
Total Tuition and Fees	120,000	-	300,000	-	480,000	-	660,000	-
Grants								
Contracts								
Other Revenues (specify)								
Total	120,000	-	300,000	-	480,000	-	660,000	-

Note: All of the above figures are estimates based on projections made by the institution submitting the proposal.

STANDARD ACADEMIC PROGRAM CHANGES
BUDGET FORM: Page 2 of 3

Use this form for programs that can be pursued on a full-time basis or through a combination of full-time and part-time attendance

EXPENDITURE ESTIMATES

	Year 1 20__		Year 2 20__		Year 3 20__		Year 4 20__	
	Additional resources required for progam	Expenditures from current resources	Additional resources required for progam	Expenditures from current resources	Additional resources required for progam	Expenditures from current resources	Additional resources required for progam	Expenditures from current resources
Personnel Services								
Administrators								
Faculty	133000		133000		133000		133000	
Support Staff			45000		45000		45000	
Others								
Fringe Benefits ____%	21481		39971		39971		39971	
Total Personnel	154,481	-	217,971	-	217,971	-	217,971	-
Operating Expenses								
Instructional Resources	10000		10000		10000		10000	
Other (specify)	24000.48		24000.48		24000.48		24000.48	
Total Operating Expenses	34,000	-	34,000	-	34,000	-	34,000	-
Capital								
Facilities								
Equipment								
Other								
Total Capital	-	-	-	-	-	-	-	-
Net Student Assistance								
Assistantships								
Fellowships								
Stipends/Scholarships								
Total Student Assisstance	-	-	-	-	-	-	-	-
Total Expenditures	188,481	-	251,971	-	251,971	-	251,971	-

Note: All of the above figures are estimates based on projections made by the institution submitting the proposal.

STANDARD ACADEMIC PROGRAM CHANGES
BUDGET FORM: Page 3 of 3

Use this form for programs that can be pursued on a full-time basis or through a combination of full-time and part-time attendance

BUDGET SUMMARY OF COMBINED EXISTING AND NEW PROGRAM

	Year 1 20__	Year 2 20__	Year 3 20__	Year 4 20__
Total revenue	120,000	300,000	480,000	660,000
Total expenses	188,481	251,971	251,971	251,971
Excess/Defeciency	(68,481)	48,029	228,029	408,029

BUDGET SUMMARY OF EXISTING PROGRAM ONLY

	Year 1 20__	Year 2 20__	Year 3 20__	Year 4 20__
Total revenue	-	-	-	-
Total expenses	-	-	-	-
Excess/Defeciency	-	-	-	-

BUDGET SUMMARY OF NEW PROGRAM ONLY

	Year 1 20__	Year 2 20__	Year 3 20__	Year 4 20__
Total of newly generated revenue	120,000	300,000	480,000	660,000
Total of additional resources required for program	188,481	251,971	251,971	251,971
Excess/Defeciency	(68,481)	48,029	228,029	408,029

Note: All of the above figures are estimates based on projections made by the institution submitting the proposal.

Appendix A Budget Justification

1 Overall

This budget is for the new PSM, and for the existing Graduate Certificate programs in Digital Forensics and in Cyber Security that will be offered using the same instructional resources as the new PSM. The attached budget shows a deficit in Year 1, which the URI Digital Forensics and Cyber Security Center will cover from existing funds in account 101-2127-0000 that are from its current Graduate Certificate programs in Digital Forensics and in Cyber Security. The program is expected to be self-sustaining (in fact profit-generating) by Year 2.

2 Revenue

Two Year Degree In Four Year Budget Form. This PSM program is a 9 course degree with each 4-credit course costing $2500. A full-time student could complete this PSM in one year. The budget form provided by the BOG seems to assume a 4-year program and the required spreadsheet does not allow changes. Since a student in this degree program could take three years (if done part-time), we used the model of the student taking one course per semester including summers, which is 3 courses per year for 3 years. Note however that this makes the revenue in Year 4 incorrect since it assumes students from Year 1 are still in the program, which is not the case in our 3-year program. Again, the required spreadsheet does not allow changes, so revenue shown in Year 4 should have $120,000 deducted from it.

Number of New Students. The number of new students shown in the BOG spreadsheet is 16 in Year 1 and 24 in subsequent years. This number reflects that we already draw 15-20 students in our Graduate Certificate programs so we expect this number to at least stay the same across all programs when there is also a PSM program available. Note that the 16 students is over all three programs: the two Graduate Certificates and the PSM. That is, our projection is that the PSM will allow the status quo in number of new students that we have seen for years in the Graduate Certificate programs – we are not assuming any increase enrollment over all three programs in Year 1 – which is conservative. After a year of traction, we expect an increase in enrollment to 24 students/year after Year 1 over the three programs.

Note that since the in-state and out-state tuition is the same in this program ($625/credit, which is what we have used in the Graduate Certificate program for years and is the result of constantly upgraded market surveys and our experience in recruiting students), that the revenue does not depend on in-state/out-state assumptions. In the BOG budget spreadsheet we assume about half in-state and half out-state; past years in the Graduate Certificate programs shows this assumption to be reasonable.

3 Expenses

Personnel.

- *One new full-time instructor.* This instructor will teach 6-8 of the courses and provide continuity to the program. The instructor will be hired on yearly contracts with a starting salary of

$65,000, which is approximately the salary of the new Instructor hired by the Computer Science Department.

- *Seven per-course adjuncts.* In a Professional Science Master's in this high-demand field, qualified adjuncts are essential to deliver the specialized courses. Our proposed model has 7 of the PSM courses being delivered by adjuncts. The typical salary for an adjunct in a fully-enrolled course is $6,000/course, which is what we typically pay adjuncts in our existing Certificate programs.
- *Two Coordinators.* The current Graduate Certificate program is coordinated by two full-time faculty members, one for Digital Forensics, and one for Cyber Security, who do this as an overload. These faculty members recruit and manage the adjuncts (and now the Instructor), determine program and course content, lead in marketing, and have done student recruitment and advising. Since we expect this PSM to mostly usurp the Graduate Certificate programs, these two positions will be responsible for doing these things in the Graduate Certificate programs and in the two tracks in the new PSM program.
- *One Support Staff.* A staff position is included after Year 1 to manage the program. The role of the Manager is described in detail in the main proposal. Essentially, the Manager will perform industry-specific marketing to attract professional students, will manage the industrial relationships that are essential to the Internship component, will manage Teaching Assistants and their hiring, will manage the budget and contracting logistics, and will perform first-level responses to program inquiries. The budget allocates $45,000 for a full-time staff position.
- *Fringe Benefits.* The fringe is based on an estimate of $21,481 for the Instructor and $18,490 for the Manager, using URI Human Resources typical formulas. The per-course adjuncts don't receive fringe and the Coordinators are full-time faculty on overload who already have fringe support.

Operating Expenses.

- *Instructional Resources.* There is $10,000/year in the budget to allow the purchase of licenses to the software tools used by the cyber security industry so that these tools are available for instruction.
- *Other.* The Other category is for Teaching Assistants. The budget allocates 12 hours per week for 6 courses per year at a rate of $23.81 for graduate students to assist the instructors in lab-intensive courses that require substantial help sessions for students.

4 Budget Summary Page

- *Year 1.* The BOG spreadsheet budget Summary shows a deficit of $68,481 for Year 1. This will be covered by the Digital Forensics and Cyber Security Center from account 101-2127-0000 that currently has those funds.
- *Subsequent Years.* The BOG spreadsheet budget shows profit in all years after Year 1. The URI DFCSC will split program profits with URI General funds and/or CCE Special Programs as specified in the included Memorandum of Understanding.

Memorandum of Understanding For Delivering Cyber Security and Digital Forensics Programs

This document outlines the responsibilities and budgeting for running the following URI programs:

- Graduate Certificate in Digital Forensics (existing)
- Professional Certificate in Digital Forensics (existing)
- Graduate Certificate in Cyber Security (existing)
- Professional Certificate in Cyber Security (existing)
- Professional Science Cyber Security Masters Degree (new)

Responsibilities

URI Digital Forensics and Cyber Security Center (DFCSC):

- Recruit Lecturer, per-course Instructors, Teaching Assistants, Manager, Coordinators
- Contract Lecturer, Manager, Teaching Assistants
- Advise students and degree accounting
- Deliver courses
- Maintain teaching facilities (online, software, etc)
- Advertise and recruit students
- Process applications
- Provide facilities for instructors, coordinators, TAs, etc

URI CCE Special Programs (CCE):

- Contract per-course instructors, Coordinators
- Handle revenue (student payment issues, etc)
- Course listings
- Administrative program management (revenue distribution)
- Advertise and recruit students
- Student billing and tuition waivers

Tuition Waivers

- Tuition waivers will be granted in a course section only if there are at least 10 paying students in that section.
- Tuition waivers are limited to 5 per course per section

Revenue distribution (see associated spreadsheet)

- CCE gets revenue for its direct costs (salaries for per-course Instructors and Coordinators)
- CCE gets 30% indirect on those direct costs provided that the DFCSC does not face a yearly deficit. If the DFCSC has a yearly deficit, CCE will reduce its indirect costs to the point of the DFCSC having no deficit or the total amount of the indirect costs, whichever is lower.
- DFCSC gets revenue for the Lecturer and Manager salaries and benefits, TA hourly, fixed software budget (e.g. $10K/year)
- Any profit over all programs listed above is allocated:
    - CCE 30%.
    - DFCSC 70%

This agreement may be revoked or altered by either party by mutual agreement with not less than one calendar year notice.

2/20/15

Victor Fay-Wolfe, Director URI Digital Forensics
And Cyber Security Center

Date

Lori E. Ciccomascolo

2/20/15

Signature URI CCE Special Programs

Date

Lori Ciccomascolo Dean, College of Continuing Education

CCE Representative Printed Name and Title

From: Elaine <efinan@mail.uri.edu>
Subject: **Assessment Plan approved: Cybersecurity MS, ONLINE**
Date: November 25, 2014 12:42:45 PM EST
To: Lisa DiPippo <dipippo@cs.uri.edu>
▶ 1 Attachment, 127 KB

Good afternoon, Lisa,

On behalf of the Office of Student Learning, congratulations on the thoroughness of your assessment documentation for the Cybersecurity MS, ONLINE. The inclusion of a Graduate Program Assessment Plan compliments the program proposal and is evidence of the program's commitment to reflection and program improvement. The Plan clearly articulates overarching program goals and learning outcomes for students, displays a curricular framework which should ensure students will have the opportunity to develop and practice the knowledge and skills necessary for success at the conclusion of the degree, and defines the use of multiple metrics for evaluating the success of the program.

I wish you the very best in your next steps toward program approval.

Best regards,

Elaine

Elaine Finan
Assistant Director
Division of Student Learning, Outcomes Assessment and Accreditation
Office for the Advancement of Teaching and Learning
University of Rhode Island, Edwards Hall
64 Upper College Road, Kingston, RI 02881
401-874-9503
web.uri.edu/assessment

GradProg-As...doc (127 KB)

THE
UNIVERSITY
OF RHODE ISLAND
COLLEGE OF
ARTS AND SCIENCES

THINK BIG WE DO℠

OFFICE OF THE DEAN
257 Chafee Social Science Center, 10 Chafee Road, Kingston, RI 02881 USA p: 401.874.4101 f: 401.874.2892 uri.edu/artsci

TO: Faculty Senate

FROM: Winifred Brownell, Dean
College of Arts and Sciences Winifred Brownell

DATE: December 11, 2014

SUBJECT: Cyber Security Professional Science Master's Degree Funding

The Arts and Sciences Dean's Office has approved the Department of Computer Science and the Digital Forensics and Cyber Security Center Proposal for a Cyber Security Professional Science Master's Degree contingent upon securing funding for the lecturer.

THE
UNIVERSITY
OF RHODE ISLAND
GRADUATE SCHOOL

APPROVAL DATE:
LOOC______________

Graduate Program Student Learning Outcomes Assessment Plan For Accredited and Non-Accredited Programs

The Graduate School requests that each program have clearly articulated program goals (Section I) and student learning outcomes statements linked to curriculum and course experiences/requirements (Section II). This assessment plan will help programs determine the extent to which these outcomes are successfully being met through courses and other program requirements. As part of the plan, each program will also create an assessment timeline (Section III) indicating when and how learning outcomes assessment will take place.[i] [ii]

Program Information:

Program:	Cyber Security Professional Science Master's Degree
Academic year plan submitted:	Fall 2014
Degree(s):	Master's Degree
Department Chair:	Joan Peckham
Program Director:	Lisa DiPippo
Accredited Program[ii]:	☒**No** □**Yes, next accreditation report due:**
Published learning outcomes (provide URL):	Not yet since this is a new program

I. Program Goals:

Broad, general statements of what it means to be an effective program in terms of student learning outcomes; what the program wants students to know and be able to do upon completion of the program. Goals should relate to the mission of the department, college, and university in which the program resides. Success in achieving Goals is evaluated directly or indirectly by measuring specific outcomes (Section II) related to the goal.

#1	Graduates can identify, manage and control vulnerabilities and threats to an organization's computer systems and networks.
#2	Graduates can diagnose attacks and define appropriate controls to mitigate attacks.
#3	Graduates can communicate and work in teams to address information security issues in a professional setting.

*Add lines as necessary

[i] If you have questions or need assistance, please contact:
Office of Student Learning, Outcome Assessment, and Accreditation, 874-9517; 874-9379.

[ii] Accredited programs can provide supplemental documents that indicate the answers to these questions as long as specific page references are provided in each cell of the tables in this form. When the answers are not accessible in that way, cutting and pasting will be required.

Graduate Program Student Learning Outcomes Assessment Plan
For Accredited and Non-Accredited Programs

II. Curriculum Mapping:

Across the top of the matrix, list courses and other requirements for the program. Order the requirements from left to right in rough chronological sequence, and append a standard description of your program requirements. Down the side, list programmatic student learning outcomes associated with goals. Using the map key below, indicate the degree to which an outcome will be taught and assessed in relevant courses and by other program requirements.

Program:

Map Key
I = Outcome Introduced
R = Outcome Reinforced
E = Outcome Emphasized

Course Numbers/Program Requirements:
In addition to specific courses, this can include internships, portfolios, and other requirements not associated with a course number, such as thesis/dissertation proposals, thesis/dissertation defenses, and comprehensive examinations.

Student Learning Outcomes (Competencies) by Goal:
Statements of observable, measurable results of the educational experience, linked to program goals (Section I), that specify what a student is expected to know or be able to do throughout a program; these must be detailed and meaningful enough to guide decisions in program planning, improvement, pedagogy, and practice.

		Core Requirements				Security Track			Both Tracks		Forensics Track					
		CSF 430	CSF 432	CSF 580	CSF 590	CSF 534	CSF 538	CSF 536	CSF 524	CSF 410	CSF 512	CSF 414	CSF 516			
Goal #1	1.1 Identify threats to the critical information assets of an organization	I	R			E	E	E								
	1.2 Characterize privacy, legal and ethical issues of information security	I/E		R	E											
	1.3 Manage, control and mitigate risk to critical information assets	I	R			R		R	E							
	1.4 Identify vulnerabilities in an organization's computer systems and networks		I			R	R		E							
Goal #2	2.1 Define the security controls sufficient to provide a required level of confidentiality, integrity, and availability in an organization's computer systems and networks	I	R			R		E								
	2.2 Diagnose attacks on an organizations computer systems and networks and propose solutions including development, modification and execution of incident response plans								E	I	R	R	R			
	2.3 Apply critical thinking and problem-solving skills to address current and future attacks on an organization's computer systems and networks		I	R	E	E	E	E	E	I	E	E	E			
Goal #3	3.1 Communicate, orally and in writing, proposed information security solutions to technical and non-technical decision-	I/E		R	E				E		E					

	makers in an organization															
	3.2 Apply business principles to analyze and interpret data for planning, decision making, and problem solving in an information security environment	I		R	E											
	3.3 Motivate and organize collaborative teams and facilitate group work in an information security environment	I		R	E											

*Add lines as necessary

Graduate Program Student Learning Outcomes Assessment Plan
For Accredited and Non-Accredited Programs

III. Assessment Timeline: Indicates when and how student learning will be assessed based on clear statements of learning outcomes and expectations. Refer to the curriculum map to draft a student learning outcomes assessment timeline. Specify a 6-year plan for assessment (3 two-year periods) in which you will assess all of your program's Goals with at least one student learning outcome representing each Goal.

Reporting Years	Learning Outcome(s)	Course(s) and Other Program Requirements	Assessment Evidence (Direct/Indirect)	Assessment Method
	WHICH outcome(s) will you examine in each reporting period?	WHERE will you look for evidence of student learning (i.e., what course(s)/program requirements)? Designate for each outcome.	WHAT student work or other evidence will you examine in order to generate conclusions and recommendations? Designate for each requirement (may use the same evidence for multiple outcomes).	HOW will you look at the evidence? What means will you use to quantify the evidence? Designate for each source of evidence.
Assessment Reporting *Period 1* May 2017	1.1 1.2 1.3 1.4	CSF 430, CSF 534, CSF 536 CSF 430, CSF 580 CSF 430, CSF 432, CSF 536 CSF 432, CSF 534, CSF 538	1.1 CSF 430 - Homework 2 CSF 534 – Cyber Challenge CSF 536 – Cyber Challenge 1.2 CSF 430 – Homework 3 CSF 580 – Final Exam 1.3 CSF 430 – Homework 4 CSF 432 – Final Exam CSF 536 – Lab 2 1.4 CSF 432 – Lab 2 CSF 534 – Cyber Challenge CSF 538 – Final Report	Rubrics designed by instructor, approved by program coordinators.
Assessment Reporting *Period 2* May 2019 (2 years later)	2.1 2.2 2.3	CSF 430, CSF 432, CSF 534, CSF 536 CSF 524, CSF 512, CSF 516 CSF 432, CSF 410, CSF 580	2.1 CSF 430 - Midterm CSF 432 - Midterm CSF 534 – Cyber Challenge CSF 536 – Final Exam 2.2 CSF 524 – Final Exam CSF 512 – Cyber Challenge CSF 516 – Final Exam 2.3 CSF 432 – Cyber Challenge CSF 410 – Cyber Challenge CSF 580 – Capstone Project	Rubrics designed by instructor, approved by program coordinators.

Assessment Reporting ***Period 3*** **May 2021** **(2 years later)**	3.1 3.2 3.3	CSF 430, CSF 580, CSF 590, CSF 524 CSF 430, CSF 580, CSF 590 CSF 430, CSF 580, CSF 590	3.1 CSF 430 – Research paper CSF 580 – Final presentation CSF 590 – Final presentation CSF 524 – Incident Response Report 3.2 CSF 430 – Homework 4 CSF 580 – Case Study Report CSF 590 – Final Report 3.3 CSF 430 – Group Case Study CSF 580 – Group Project CSF 590 – Final Report	Rubrics designed by instructor, approved by program coordinators.

LIBRARY IMPACT STATEMENT (New Program Proposal)
LIBRARIAN'S ASSESSMENT

Subject selectors will complete this form as requested, assessing library materials and collections as detailed below. Send one copy of the assessment to the faculty member who requested it. Send one copy of the assessment to the Collection Management Officer.

Program: Cyber Security Professional Science Master's Degree

Department, College: Computer Science and Statistics, A&S

Faculty Member: Lisa DiPippo

Date returned to Faculty: 10/22/14

Librarian Completing Assessment: Amanda Izenstark

Collection Management Officer: Joanna Burkhardt

Assessment of:

- Suitability of existing library resources;
- New library resources required to support the program;
- Information skills education required by the students; and
- Funds needed for library materials and services.

Please include:

1. What library holdings already exist in relevant subject categories, including supporting collections from HELIN. How much money is now allocated in the program area?

   $3,495 per year is allocated for Computer Science & Statistics monographic purchases.

   As the University already has courses in cyber security, the topics covered by the course are well supported by journal subscriptions, databases, and ebooks at URI, and by print monographs available at the University Libraries and from the HELIN consortium.

2. Does URI have the essential journals as noted in the Faculty Questionnaire?

   Yes. The library has online subscriptions to the following essential journals:

   International Journal of Information Security
   ACM Transactions on Information Systems Security
   IEEE Security & Privacy
   Information Security Journal
   Journal of Computer Security

The library also has additional online subscriptions to journals of use to students in the course, such as:

IEEE Transactions on Information Forensics and Security
IEEE Transactions on Dependable and Secure Computing

3. What new resources are required to support the program (including media, electronic, or other non-print materials)?

   No new resources are required, but the addition of an online course may necessitate adding another user to the University Libraries' Safari Tech Books Online subscription to support student research. (The Libraries' subscription currently allows for two simultaneous users.)

4. What information mastery sessions will be required for the students?

   Because most of the classes in this program rely on course materials, no formal sessions will be necessary, but because the course is online and students may be unfamiliar with the research support the University Libraries provide, an online orientation to URI-subscribed research resources is recommended. Individual consultations with students can be arranged on an as-needed basis.

5. What is the approximate cost to acquire the materials necessary? Which of these will be continuing costs?

   Adding another user to the Safari Tech Books subscription would cost approximately $1,500/year.