Addendum to the National University General Catalog 75

MODIFICATIONS TO STUDENT SUPPORT SERVICES

Technical Requirements

Headset with Microphone with USB connection

College of Letters and Sciences

Revised Course Prerequisites

Effective 8/30/2011

PSY 448	History of Sport and Sport Psychology *Prerequisite: PSY 100, PSY 302*
PSY 440	Sport Psychology for Coaches *Prerequisite PSY 100, PSY 302*
PSY 443	Culture and Sport Psychology *Prerequisite: PSY 100, PSY 302*
PSY 445	Applied Sport Psychology *Prerequisite: PSY 100, PSY 302*
PSY 442	Seminar in Applied Sport Psychology *Prerequisite: Satisfactory completion of 10 courses in the major*
PSY 485	Senior Project in Sport Psychology *Prerequisite: Satisfactory completion of ALL major requirements*
PGM 444	Instruction/Player Development *Prerequisite: Satisfactory completion of 8 core courses*
PGM 447	Prof. Golf Mgmt Seminar *Prerequisite: PGM 444*
PGM 445	Player Development II Seminar *Prerequisite: PGM 447*
PGM 448	Senior Project in PGM *Prerequisite: satisfactory completion of ALL major requirements*

SCHOOL OF EDUCATION

Course Description

SPD 604 Psychological Fdns of Educ.
An examination of learning processes in educational settings will address human motivation; development of children and youth in the affective, cognitive, social, and personal domains; individual differences; and implications of theory and research for teaching and learning.

SCHOOL OF ENGINEERING, TECHNOLOGY, AND MEDIA

PROGRAM MODIFICATION WITH NEW SPECIALIZATIONS

■ MASTER OF SCIENCE IN CYBER SECURITY AND INFORMATION ASSURANCE

Faculty Advisor: Ron Gonzales; (858) 309-3435; rgonzales@nu. edu

The Master of Science in Cyber Security and Information Assurance is a professional degree for those who endeavor through technical and managerial measures to ensure the security, confidentiality, integrity, authenticity, control, availability and utility of the world's computing and information systems infrastructure. The program has a required core and a required specialization which can be selected from some alternatives. The core is designed to provide a means of supporting the variety of backgrounds (both education and work experience) that those who wish to study this area may bring to the program. The core is also a statement of the knowledge domain that is common to most efforts in this area. The specializations provide for study in particular domains of knowledge within the field – which are also tied to communities of effort within the field.

Program Admission Requirements

All students who seek to enroll in the MS program must meet with the Faculty Advisor noted above prior to enrolling in the first course of the program. Prerequisite courses must be met or the student must secure approval from the Faculty Advisor.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Evaluate the interaction and relative impact of human factors, processes and technology in CSIA infrastructures.
- Devise a mitigation plan against both external and internal vulnerabilities to enterprise computer infrastructures and sensitive digital assets.
- Support multiple risk assessment strategies and processes to maximize effectiveness and minimize costs of CSIA in a high assurance information system.
- Integrate systems-level-infrastructure thinking into CSIA problem identification and resolution, and effectively communicate the solution.
- Differentiate among the models, architectures, challenges and global legal constraints of secure electronic commerce technologies used to ensure transmission, processing and storage of sensitive information.
- Prescribe how to provide message privacy, integrity, authentication and non-repudiation using network security practices and infrastructure hardening techniques.
- Evaluate and contrast the impact of diverse ethical perspectives, cultural customs and organizational political dynamics on CSIA.
- Assess, from both a national and global perspective, the relative demands of Internet-openness, legislation and law-enforcement, and individual right-to-privacy.
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA.
- Conduct in-depth research into a specific CSIA topic, including finding and integrating relevant research results of others.
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments.
- Integrate project development skills in producing a security system.

Degree Requirements

To obtain the Master of Science in Cyber Security and Information Assurance, students must complete 54 graduate units. A total of 13. 5 quarter units of graduate credit may be granted for equivalent graduate work completed at another regionally accredited institution, as it applies to this degree, and provided the units were not used in earning another advanced degree. All students must complete the 8 core requirements and choose an Area of Specialization. Please refer to the graduate admissions requirements for specific information regarding application and evaluation.

Core Requirements

(8 courses: 36 quarter units)

CYB 600	Cyber Security Technology
CYB 601	Cyber Sec. Toolkit Utilization *Prerequisite: CYB 600 with a minimum grade of B*

CYB 602	Threat Mitigation Policy/Audit *Prerequisite: CYB 601*
CYB 603	Cyber Security Ethical Issues *Prerequisite: CYB 602*
CYB 604	Wireless and Mobile Security *Prerequisite: CYB 603*
CYB 605	Information Assurance Part I *Prerequisite: CYB 604*
CYB 606	Net Defense & Countermeasures *Prerequisite: CYB 605*
CYB 699	Cyber Policy Project *Prerequisite: CYB 606 and completion of one specialization area*

Requirements for the Specializations
(4 courses; 18 quarter units)

All students must choose one Specialization defined below:

▲ Specialization in Health Information Assurance

The specialization in Health Information Assurance provides study in the professional domain of Cyber Security and Information Assurance that seeks to apply the concepts and practices of this field to a specific industry domain - Health. This domain has sensitive information on individuals and depends on this information for its practice so security in this industry is particularly important.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Differentiate among the models, architectures, challenges and global legal constraints of secure electronic commerce technologies used to ensure transmission, processing and storage of sensitive information. (PLO 5)
- Prescribe how to provide message privacy, integrity, authentication and non-repudiation using network security practices and infrastructure hardening techniques. (PLO 6)
- Assess, from both a national and global perspective, the relative demands of Internet-openness, legislation and law-enforcement, and individual right-to-privacy. (PLO 8)
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA. (PLO 9)
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments. (PLO 11)
- Produce a successful project using project development skills. (PLO 12)
- SPECIALIZATION: Prepare a health information risk mitigation and security plan.
- SPECIALIZATION: Propose information privacy policies that maintain the confidentiality of personal data in health care.
- SPECIALIZATION: Prescribe information assurance requirements for Health care.

Degree Requirements:

This specialization requires 18 graduate units at National University.

Program Requirements

(4 courses; 18 quarter units)

CYB 611	Cyber Sec. Mgmt & Cryptography *Prerequisite: CYB 606*
CYB 613	Information Assurance Part II *Prerequisite: CYB 605*
CYB 614	Privacy of Information *Prerequisite: CYB 611*
CYB 615	Info Assurance of Med. Records *Prerequisite: CYB 614*

▲ Specialization in Computer Forensics

The specialization in Computer Forensics provides study in the professional domain of Cyber Security and Information Assurance that seeks to build and present facts about computer and network usage generally for the purposes of explaining what has happened and holding those responsible to account. This requires particular attention to servers as well as clients, and particularly data servers.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Differentiate among the models, architectures, challenges and global legal constraints of secure electronic commerce technologies used to ensure transmission, processing and storage of sensitive information. (PLO 5)
- Prescribe how to provide message privacy, integrity, authentication and non-repudiation using network security practices and infrastructure hardening techniques. (PLO 6)
- Assess, from both a national and global perspective, the relative demands of Internet-openness, legislation and law-enforcement, and individual right-to-privacy. (PLO 8)
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA. (PLO 9)
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments. (PLO 11)
- Produce a successful project using project development skills. PLO 12)
- SPECIALIZATION: Organize a functional forensic security tool kit.
- SPECIALIZATION: Derive a network usage history, identify and characterize event origins, and recreate the chronology of events.
- SPECIALIZATION: Create an application of forensic principles for SQL Server databases.

Degree Requirements

This specialization requires 18 graduate units at National University.

Program Requirements

(4 courses; 18 quarter units)

CYB 611	Cyber Sec. Mgmt & Cryptography *Prerequisite: CYB 606*
CYB 621	Computer Forensics Principles *Prerequisite: CYB 611*
CYB 622	Computer Forensics Technology *Prerequisite: CYB 621*
CYB 623	SQL Serv. Forensics Principles *Prerequisite: CYB 622*

▲ Specialization in Information Assurance and Security Policy

The specialization in Information Assurance and Security Policy provides study in the professional domain of Cyber Security and Information Assurance that focuses on the organizational and informational portion of the field. This arena particularly involves larger organizations, often in government, that have codified standards, policies and practices for this field.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:

- Differentiate among the models, architectures, challenges and global legal constraints of secure electronic commerce technologies used to ensure transmission, processing and storage of sensitive information. (PLO 5)
- Prescribe how to provide message privacy, integrity, authentication and non-repudiation using network security practices and infrastructure hardening techniques. (PLO 6)
- Assess, from both a national and global perspective, the relative demands of Internet-openness, legislation and law-enforcement, and

individual right-to-privacy. (PLO 8)
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA. (PLO 9)
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments. (PLO 11)
- Produce a successful project using project development skills. (PLO 12)
- SPECIALIZATION: Prepare an IT risk mitigation and security plan.
- SPECIALIZATION: Prepare and create an enterprise disaster recovery and business continuity plan.
- SPECIALIZATION: Derive information assurance from an INFOSEC perspective.

Degree Requirements:

This specialization requires 18 graduate units at National University.

Program Requirements

(4 courses; 18 quarter units)

CYB 611	Cyber Sec. Mgmt & Cryptography *Prerequisite: CYB 606*
CYB 612	Disaster Rec. /Bus. Continuity *Prerequisite: CYB 611*
CYB 613	Information Assurance Part II *Prerequisite: CYB 605*
CYB 616	Info Assurance/INFOSEC Posture *Prerequisite: CYB 613*

▲ Specialization in Ethical Hacking & Pen Testing

The Ethical Hacking & Pen Testing specialization is designed to provide unique applications involved in the professional domain of Cyber Security and Information Assurance. The curriculum focus is directed toward ethical hacking and penetration testing. Penetration tests probe network and information system security components by conducting simulated attacks on systems. This specialization prepares the professional to develop rules of engagement, prepare a tool kit, discover and exploit system vulnerabilities, ethically conduct a pen test and prepare pen test documentation. Red Teaming practices are utilized and Red vs. Blue team exercises are executed.

Program Learning Outcomes

Upon successful completion of this program, students will be able to:
- Devise a mitigation plan against both external and internal vulnerabilities to enterprise computer infrastructures and sensitive digital assets. (PLO 2)
- Integrate systems-level-infrastructure thinking into CSIA problem identification and resolution, and effectively communicate the solution. (PLO 4)
- Forecast the impact of continually advancing technology and national and international cyber-legislation on CSIA. (PLO 9)
- Conduct in-depth research into a specific CSIA topic, including finding and integrating relevant research results of others. (PLO 10)
- Generate critical thinking in analysis and synthesis of enterprise and global CSIA issues through effective individual and team graduate-level written and oral assignments. (PLO 11)
- Integrate project development skills in producing a security system. (PLO 12)
- SPECIALIZATION: Produce a pen test authorization and rules of engagement document.
- SPECIALIZATION: Prepare and synthesize process specifications of Red Team actions against a Blue Team defense of a computer infrastructure.
- SPECIALIZATION: Prepare and synthesize process specifications of a Blue Team defense used to protect the computer infrastructure against a Red Team attack

Degree Requirements

This specialization requires 18 graduate units at National University.

Program Requirements

(4 courses; 18 quarter units)

CYB 611	Cyber Sec. Mgmt & Cryptography *Prerequisite: CYB 606*
CYB 632	Info Sys Vulnerab & Attacks *Prerequisite: CYB 611*
CYB 633	Red Teaming *Prerequisite: CYB 632*
CYB 634	Red vs. Blue Team Exercise *Prerequisite: CYB 633*

New Courses

CYB 632 Info Sys Vulnerab & Attacks

Prerequisite: CYB 611

Students will apply principles of penetration testing to identify and exploit vulnerabilities in network facing information systems and make recommendations for mitigation. This course uses tools such as the Metasploit Framework that is a free, open source penetration testing solution developed by the open source community.

CYB 633 Red Teaming

Prerequisite: CYB 632

Red Teaming, or Alternative Analysis, is the practice of viewing a problem from an adversarial or competitor's perspective. The objective of Red Teams is to enhance decision making, practices of secured system protection applicable by establishing countermeasures of defense. A contributing outcome of this course to the entire MS CSIA program is to help students employ actively open-minded/problem solving, unbiased thinking to CSIA.

CYB 634 Red vs. Blue Team Exercise

Prerequisite: CYB 633

Students will analyze and perform Red vs. Blue Team objective-based cyber operations as an active approach to establish a defensive posture improvement. The basic idea of Red vs. Blue team countermeasures is simple – war gaming. A virtual enterprise computer infrastructure is established and the Red Team will attack the infrastructure, whereas, the opposing Blue Team will defend against the attack. This level of risk management has been actively deployed in both government and industry. This exercise prepares the student for the final team project in MS CSIA course CYB 699.

SCHOOL OF HEALTH AND HUMAN SERVICES

The following programs require ALL Nursing (NSG) courses to be taken in the order listed in catalog 75 (not including General Education Courses):

■ BACHELOR OF SCIENCE IN NURSING (BSN) (CALIFORNIA) – GENERIC ENTRY

Page 314 - Preparation for the Major and Nursing Core Courses

■ LICENSED VOCATIONAL NURSE TO BACHELOR OF SCIENCE IN NURSING (LVN TO BSN) (CALIFORNIA)

Page 313 - Nursing Core Courses

■ BACHELOR OF SCIENCE IN NURSING (BSN) ACCELERATED POST-BACHELOR DEGREE (CALIFORNIA)

Page 311 - Preparation for the Major and Nursing Core Courses www.nu.edu