Graduate Catalog Addendum/Errata

Below are listed additions and/or corrections to the 2013-14 Graduate Catalog since its publication on June 1, 2013. All corrections listed below have been made in the main online catalog sections to which they apply and will appear in the print version of those individual pages. They do not appear, however, in the PDF version of the full catalog. The last day for corrections in this catalog was October 31, 2013.

Changes by Dept/Program:

- Academic Policies/Sequential Master's Degree
- Accreditation Memberships/Licensures/Approvals and Specialized Accreditaitons
- Applied Educational Psychology: School Psychology (EdS)
- Cybersecurity (MS) (New Program)
- EPSY 6200 Seminar in School Psychology
- ESOL Certification
- Global MA in International Relations
- Master of Business Administration (MBA)
- Mathematics for Educators (MAT)
- Public Relations (MA)
- School of Education
- Tuition, Fees and Refunds/Payment Requirements
- U.S. Patent Practice (MS)

be EPSY instead of ESPY:

Goal 2 Professional Practice Preparation (10 hours) should read:

- EPSY 6121 Portfolio Based Analysis: School Psychology (2)
- EPSY 6100: Practicum in Data-Based Decision-Making: Mental Health Services (2)
- EPSY 6100: Practicum in Data-Based Decision-Making: Advanced Psychoeducational Assessment and Intervention (2hours)
- EPSY 6500 School Psychology Internship (4 hours)

Goal 5 Research Methods and Statistical Skills (5 hours) should read:

- EPSY 6100: Practicum in Data-Based Decision-Making: Consultation and Applied Field Research (1 hour)
- EPSY 6000 Advanced Graduate Certificate Project (3 hours)

Changes by Date:

June 17, 2013

Course Descriptions/EPSY

EPSY 6200 was updated to read:

The purpose of EPSY 6200 Seminar in School Psychology is to assist in the preparation of school psychology graduate students for entry into the field. The seminars include topics and activities in the professional practice of school psychology.

Seminars in School Psychology: Professional School Psychology (2) . This seminar is designed to familiarize students with the roles and functions of the school psychologist in school settings or other alternative service delivery systems. Topics include assessment, consultation, intervention, special education, research, ethics and standards, and the future of education and school psychology.

Seminars in School Psychology: International and Multicultural Perspectives (2) . This seminar is designed to provide international and multicultural perspectives on the roles and functions of the school psychologist. Topics include the following: the international growth in school psychology, cultural diversity, global perspectives, social justice, children’s rights, effects of poverty, professional organizations, and the future of school psychology.incorrect. The list below reflects the correct prefixes, which should

tuition, zero-credit-hour course in which students write an essay describing how they have changed as a result of participating in the program.

Public Relations (MA)

The list of Elective Courses should read:

A minimum of 15 credit hours must be completed from the following:

- ADVT 5321 Advertising Decision-Making (special prerequisites) (3 hours)
- MEDC 5010 Introduction to Graduate Studies: Advanced Thinking and Writing (3 hours)
- MEDC 5300 Strategic Communications (3 hours)
- MEDC 5343 Writing for Media Communications: Scriptwriting (3 hours)
- MEDC 5345 Writing for Media Communications: Journalism (3 hours)
- MEDC 5400 Media Production Management (3 hours)
- MEDC 5430 Media Communications Technology (3 hours)
- MEDC 5460 Media Resear.37edia Resear.37es)

knowledge, and critical thinking skills to practice the art and science of Cybersecurity management.

Students entering the Cybersecurity program should have knowledge of computer systems, digitalnetworks, familiarity with internet and wireless applications, and possess good (high school algebra and exposure to trigonometry) mathematical as well as written and oral communication skills.

The M.S. in Cybersecurity prepares individuals for demanding positions in public and private sectors overseeing, operating, or protecting critical computer systems, information, networks, infrastructures and communications networks.

Students will be well-versed to apply their knowledge and critical thinking related to domestic and international legal systems, private and public policies, and ethics, as they apply cybersecurity to, information protection, terrorism, fraud, theft, intelligence/ counterintelligence, digital forensics, pre-emptive and strategic force operation application situations.

Program Learning Outcomes

1. a.

and applying counterintelligence to evade, trick or trap individuals, agencies, or national entities who wish to steal, damage or deny access to valid users of critical information and its sources. Active measures, passive counter measures, and intelligence gathering processes as well as determining the validity and success of gathering information will be included. Prerequisite：CSSS 5000

CSSS 5140 Cybersecurity Strategic Operations (3)

Specific methods, ethics, laws, policies and procedures for conducting strategic operations and countermeasures are the focus of this course. Students will learn how to identify critical infrastructures, communication channels, and information protection schemes and how to detect threats, assess vulnerabilities, penetrate and exploit cyber targets, understand how to monitor, spoof, redirect and deny access, as well as protect critical assets. Prerequisite: CSSS 5000

CSSS 5210 Cybersecurity Law and Policy (3)

The laws and policies dealing with cyber-crime, cyber warfare, privacy and international perspectives as well as an in depth look at the National Security Act, the United States Cybersecurity Electronic Security Act, the Cyber Security Enhancement Act, the Protecting Cybersecurity as a National Asset Act, the Communications Assistance for Law Enforcement Act (CALEA), cyber-crime laws, international cyber-crime laws and other current laws and policies will be reviewed and discussed. Prerequisite: CSSS 5000

CSSS 5220 Cybersecurity Threat Detection (3)

Students will examine various methods used to threaten our Cyber systems such as: viruses; spoofing; denial of service; fraud; theft; phishing; spy bots; spam; Trojan horses; email and active malware attachments; viral applications; hardware (computers and portable storage devices) with built in viruses or trap-doors; fake web sites; as well as eaves dropping via wireless networks; criminal access to national, corporate or personal data; and the growing loss of privacy over social networks. Prerequisite：CSSS 5000

CSSS 5230 Cybersecurity Forensics (3)

The course covers methods and procedures for identification and recovery of damaged or erased digital data, tracing information access (web history, cookies, cache memory and internet source identification), determination of system vulnerabilities (e.g., TEMPEST), communication ports and computer system architectures and encryption methods, as well as incident monitoring and response. Prerequisite：CSSS 5000

CSSS 5240 Pre-Emptive Deterrence (3)

This course addresses specific methods, ethics, laws, policies and procedures for planning and executing pre-emptive Cybersecurity deterrence operations and force application. Prerequisite: CSSS 5000

CSSS 5250 Use and Protection of Space Assets (3)

A unique course, it focuses on all three segments (space, ground and user) of fixed and mobile communication and Global Positioning System (GPS) assets and their attributes. Secure and non-secure systems are examined to show the breadth of capabilities along with the pros and cons. Uplink and downlink signal characteristics, signal bouncing and relaying capabilities. Frequency hopping, spread-spectrum, interception and overpowering of signals through use of steerable beams, application of laser and fiber-optics, and encryption techniques are cover. Prerequisite：CSSS 5000

CSSS 5260 Encryption/Decryption Methods and Techniques (3)

The history and application of ciphers, codes and encryption/decryption methods and techniques are examined in detail. Public and Private keys and other advanced methods will be included. Understanding the overhead of encryption on communications systems and the storage of data as well as methods employed for decryption, verification and authentication. Aspects of ethics and information privacy have a role when security is applied to public systems and email content as well as higher levels of security for corporations proprietary and government classified information; additionally, the Data Protection Act will be discussed. Prerequisite：CSSS 5000

CSSS 5990 Advanced Topics in Cybersecurity (3)

This course is designed to permit addressing advanced and emerging topics in Cybersecurity that may include, but not be limited to, Cybersecurity communications, cyber warfare planning and execution, forensics, ethics, policies and laws, encryption/decryption and future topics e.g., application of quantum non-locality. This course may be repeated for credit if the content differs. Prerequisite：CSSS 5000

CSSS 6001 Practical Research in Cybersecurity I (3)

The student is expected to synthesize and integrate the learning experiences acquired throughout the MS in Cybersecurity and to evaluate current and future topics relative to this major. Prerequisite: successful completion of all required core courses in this major and declaration of the thesis option in accordance with the thesis policy (as applicable). Specific papers, projects, or other methodologies must include Cybersecurity related technical and management areas than span this entire degree emphasis. Internships or practical research projects that span two consecutive semesters are considered appropriate applications of student research in conjunction with the completion of this course. Prerequisite: All CSSS Core Courses

CSSS 6002 Practical Research in Cybersecurity II (3)

The student is expected to synthesize and integrate the learning experiences acquired throughout the MS in Cybersecurity and to evaluate current and future topics relative to this major. Prerequisite: successful completion of all required core courses in this major and declaration of the thesis option in accordance with the thesis policy (as applicable). Specific papers, projects, or other methodologies must include Cybersecurity related technical and management areas than span this entire degree emphasis. Internships or practical research projects that span two consecutive semesters are considered appropriate applications of student research in conjunction with the completion of this course. Prerequisite：CSSS 6001

October 29, 2013

Tuition, Fees and Refunds/Payment Requirements

The third paragraph has been revised to read:

Students are encouraged to make electronic check payments online, but personal checks made payable to Webster University are also accepted. A $30 returned payment fee is charged if payment is returned. Webster also accepts MasterCard, Discover, VISA, and American Express payments online with a 2.75% convenience fee.