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)

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.

July 19, 2013

Global MA in International Relations

In the **Program Curriculum** section, the course number for Professional Seminar was corrected to
INTL 5500

.

July 31, 2013

Academic Policies/Sequential Master's Degree

The list of Sequential Master's Degrees should include:

minimum 30 credit hours required for:

- MS in Forensic Accounting

Applied Educational Psychology: School Psychology (EdS)

Under **EdS Program Coursework**, some course prefixes were incorrect. The list below reflects the correct prefixes, which should 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 (2 hours)
- EPSY 6500 School Psychology Internship (4 hours)

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

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

Goal 6 Knowledge of Ethics and Establishment of Professional Values (4 hours) should read:

- EPSY 6200: Seminar in School Psychology: Professional School Psychology (2 hours)
- EPSY 6200: Seminar in School Psychology: International and Multicultural School Psychology (2 hours)

Master of Business Administration (MBA)

Under emphasis in **Decision Support Systems**, a reference is made to the Graduate Certificate in Decision Support Systems. That certificate is no longer offered, and the link to that program has been removed.

Mathematics for Educators (MAT)

Requirements should read:

Mathematics students must meet the requirements for an emphasis in community college mathematics, secondary mathematics or middle school mathematics. Upon completing 9 credit hours, students are required to be advanced to candidacy. Refer to the section on Advancement to Candidacy in this catalog for specific guidelines.

During their penultimate semester, and at least one academic year following their advancement to candidacy, students need to register for MTHC 5900 Final Reflections. This is a no-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 Research (3 hours)
- MEDC 5500 Professional Seminars (1-3 hours)
- MEDC 5550 Topics in Media Communications (3-6 hours)
- MEDC 5600 Introduction to Interactive Communications (3 hours)
- MEDC 5650 Special Topics in Interactive Media (3 hours)
- PBRL 4190 Public Relations Research (3 hours)
- PBRL 4800 Media Relations (3 hours)
- PBRL 5323 Organizational Communications (3 hours)
- PBRL 5342 Writing for Public Relations (if not used as a core course) (3 hours)
- PBRL 5344 Speech Writing (if not used as a core course) (3 hours)
- PBRL 5451 Communication Strategies for Investors and Financial Stakeholders (3 hours)
- PBRL 5452 Communication Strategies for Public Affairs and Government Relations (3 hours)
- PBRL 5453 Communication Strategies for Nonprofit Organizations (3 hours)
- PBRL 5465 Crisis Management Communications (3 hours)
- PBRL 5550 Topics in Public Relations (3-6 hours)
- PBRL 5770 Multinational Public Relations (3 hours)

U.S. Patent Practice (MS)

Program Curriculum should
include PATA 5200

in the list of required courses. The list should read:

- LEGL 5000 Introduction to Legal Studies (Requisite Course) (3 hours)
- PATA 5100 Introduction to Patent Law (3 hours)
- PATA 5110 Patent Research and Writing (3 hours)
- PATA 5120 Foundations in Intellectual Property Law (3 hours)
- PATA 5200 Patent Drafting (3 hours)
- PATA 5210 Patent Prosecution (3 hours)
- PATA 5300 Patent Office Ethics (3 hours)
- PATA 5310 Patent Law Regulations and Procedures (3 hours)
- PATA 5400 Patent Litigation in the Federal Courts (3 hours)
- PATA 6000 Integrated Practices in U.S. Patent Office Procedure (3 hours)

September 8, 2013

ESOL Certification

ESOL Certification was
removed from list of Certificates

; it is not a certificate but is part of the MA in Teaching English as a Second Language

Accreditation Memberships/Licensures/Approvals and Specialized Accreditaitons

Licensure information for Washington State has been revised to:

Webster University is authorized by the Washington Student Achievement Council and meets the requirements and minimum educational standards established for degree-granting institutions under the Degree-Granting Institutions Act. This authorization is subject to periodic review and authorizes Webster University to offer specific degree programs. The Council may be contacted for a list of currently authorized programs. Authorization by the Council does not carry with it an endorsement by the Council of the institution or its programs. Any person desiring information about the requirements of the act or the applicability of those requirements to the institution may contact the Council at P.O. Box 43430, Olympia, WA 98504-3430.

School of Education

The following has been inserted, as required by NCATE:

Assessment Policy of School of Education

All programs in the School of Education use key assessments in specific courses to evaluate and promote student achievement of specific learning outcomes. In all courses that use key assessment assignments, students will see on each syllabus the standards that are used for assessing their academic performance. In addition, all faculty and students are expected to use the web-based TK20 Assessment System for the submission and evaluation of key assessment assignments; TK20 serves as the school's electronic assessment system. Students may contact their advisors, if they have further questions.

NEW PROGRAM: Cybersecurity (MS)

This program will be offered through the George Herbert Walker School of Business & Technology, beginning Spring 1, 2014:

Program Description

The Master of Science (M.S.) degree-seeking student should consult the Admission, Enrollment, and Academic Policies sections under Academic Policies and Procedures for policies regarding application, admission, registration, and the academic policies of Webster University.

Students may not apply for dual majors because of the technical nature of this M.S. degree program. Students may apply for sequential degrees as long as they do not duplicate core courses applying to their sequential degree emphasis area. The capstone course in each emphasis is required and unique to its area of emphasis.

Education at the graduate level is an expansion of the knowledge attained from undergraduate studies. Graduate education encourages the development of advanced skills, theoretical 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. Graduates will be capable of explaining important principles, and theories used throughout the field of Cybersecurity.
   b. Graduates will be capable of applying knowledge in the field of Cybersecurity to analyze real world problems.
   c. Graduates will be capable of effectively integrating knowledge in the field of Cybersecurity to propose solutions to real world problems.

Program Curriculum

The 39 credit hours required for the M.S. degree in Cybersecurity must include the required core courses.
Core Courses

- CSSS 5000 - Introduction to Cybersecurity (3)
- CSSS 5110 – Cybersecurity Communications (3)
- CSSS 5120 – Cybersecurity Infrastructures (3)
- CSSS 5130 – Cybersecurity Intelligence/Counter Intelligence (3)
- CSSS 5140 – Cybersecurity Strategic Operations (3)
- CSSS 6001 - Practical Research in Cybersecurity (3)*
- CSSS 6002 - Practical Research in Cybersecurity (3)*

*CSSS 6001 and 6002 must be taken sequentially over two terms; CSSS 6001 is a Prerequisite for CSSS 6002

Four elective courses chosen from the following:

- CSSS 5210 – Cybersecurity Law and Policy (3)
- CSSS 5220 – Cybersecurity Threat Detection (3)
- CSSS 5230 – Cybersecurity Forensics (3)
- CSSS 5240 - Pre-emptive Deterrence (3)
- CSSS 5250 - Use and Protection of Space Assets (3)
- CSSS 5260 - Encryption Methods and Techniques (3)
- CSSS 5990 - Advanced Topics in Cybersecurity (3)*

*A maximum of two CSSS 5990 – Advanced Topics in Cybersecurity courses may be counted toward the 39 required Webster Courses.

The student must also select two additional electives from CSSS or other Webster elective credit courses that may be offered at the location where the student is completing their MS requirements.

All students in this curriculum must complete the capstone courses CSSS 6001 and CSSS 6002 over two sequential terms as a practical research paper, an internship, or an individual or team project for a total of [6] credit hours and 72 contact hours. An assessment assignment is required and will be administered to each student as part of the capstone course project.

Webster reserves the right to restrict access to some courses that may require specific clearances to address specific classified topics related to advanced course content in Cybersecurity. Professors must advise the Site Director, Faculty Advisor or Site Manager of the potential of including any classified content in the course and clearly identify the need for security clearances, the level, agency issued by, and methods employed for the protection of information with applicable security policies and procedures at the location where the course is to be taught. Counselors must understand specific clearance requirements of these courses and the specific clearances of students attempting to enroll in these courses. This restriction will only apply to those programs offered at National Laboratories; Intelligence Agencies or specified Military sites which request this level of security

The following NEW COURSES associated with this degree are as follows:

CSSS 5000 Introduction to Cybersecurity (3)

This requisite course is designed to provide the student an overview of the major core areas of study they will encounter throughout this program. Introduction of computer system architectures, vulnerabilities, critical infrastructures, the growing threat of social networks, intelligence and counter intelligence, international laws, security policies, privacy and information liability, cyber attacks and counter cyber attacks, encryption, risk assessment, cybersecurity forensics including data gathering and recovery, and a forward look at future cyber technology developments.

CSSS 5110 Cybersecurity Communications (3)

Digital communications has grown rapidly and provides increased opportunities to: access information; share and disseminate knowledge; create new innovative services; and compete in a global environment. It presents new opportunities and a growing threat posed by a connected society that can impact critical United States interests. The basics of communication systems, the ISO Layer Model, topologies such as Local-Area-Networks (LANs), Wide-Area-Networks (WANs), World Wide Web and the Internet, space-based communications used by Department of Defense (DoD) and commercial entities, fiber-optics, as well as the rapidly developing personal mobile communication technologies such as Wireless Local Area Network (WiFi). **Prerequisite**: CSSS 5000

CSSS 5120 Cybersecurity Infrastructures (3)

The impact of September 11, 2001 cemented our attention on physical attacks on United States critical infrastructures. Although still a concern, a growing Cybersecurity threat requires additional focus on potential virtual attacks on these same critical infrastructures. Both physical and virtual in capacitance of a critical infrastructure such as the Power Grid, Communications, and Financial transactions can have as great, or greater, impact on our society, Cyber attacks have and can cripple an industry and the services they provide to millions of users. The critical infrastructures identified by the Department of Homeland Security (DHS) are examined from a Cybersecurity perspective. **Prerequisite**: CSSS 5000

CSSS 5130 Cybersecurity Intelligence/Counter-Intelligence (3)

Students examine methods, ethics, policies and procedures for accessing and gathering information for positive or negative use, 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.