



## BOARD OF REGENTS

### SUMMARY OF ITEM FOR ACTION, INFORMATION OR DISCUSSION

---

**TOPIC:** University of Baltimore: Master of Science in Forensic Science – High Technology Crime

**COMMITTEE:** Education Policy and Student Life

**DATE OF COMMITTEE MEETING:** January 16, 2013

**SUMMARY:** The core of the proposed M.S. degree program in Forensic Science – High Technology Crime (MSFS) exposes students to forensic investigation techniques and skills, computer and digital information crimes, financial and health care fraud, prevention and security management strategies, and legal interventions and resolutions. The program, developed in consultation with the FBI, statewide law enforcement, and the chief executive officers at Citigroup Security, is intended for members of private corporations, nonprofit organizations, and governmental agencies, who desire to advance their competencies in managing advanced technological resources to combat cyber threats, and related financial crime.

The interdisciplinary nature of the MSFS program may attract new students interested in forensic science, health care fraud, and/or forensic accounting who might not otherwise pursue graduate study at the University. The MSFS program will develop students' knowledge and skills as experts in the recognition of high technology crimes, thereby preparing them to investigate the expanding area of criminal activity relating to technology.

The most recent employment data (2010) from the Bureau of Labor Statistics affirms the demand for employees in cyber security related work, both within governments and in the public sector. In Maryland, 68,000 people are employed in security related occupations and a recent search of Indeed.com, a jobs website, indicates 342 job openings at all levels in cyber security.

**ALTERNATIVE(S):** The Regents may not approve the program or may request further information.

**FISCAL IMPACT:** No additional funding is necessary. The program will be supported through tuition.

**CHANCELLOR'S RECOMMENDATION:** That the Committee on Education Policy recommend that the Board of Regents approve the proposal from the University of Baltimore to offer the Master of Science in Forensic Science – High Technology Crime.

---

**COMMITTEE RECOMMENDATION:** Approval

**DATE:** January 16, 2013

---

**BOARD ACTION:**

**DATE:**

---

**SUBMITTED BY:** Joann A. Boughman

301-445-1992

[jboughman@usmd.edu](mailto:jboughman@usmd.edu)

---

**UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR**

- ☒ New Instructional Program  
☐ Substantial Expansion/Major Modification  
☐ Cooperative Degree Program  
☐ Within Existing Resources, or  
☐ Requiring New Resources

University of Baltimore  
Institution Submitting Proposal

**M.S. Program in Forensic Science – High Technology Crime**

Title of Proposed Program

**M.S. Program in Forensic Science – High  
Technology Crime**

**FALL 2013**

Award to be Offered

Projected Implementation Date

**[210505]**

**43.0116**

Proposed HEGIS Code

Proposed CIP Code

School of Criminal Justice  
College of Public Affairs

Debra L. Stanley, Ph.D.  
Charles Tumosa, Ph.D.

Department in which program will be located

Department Contact

(410) 837-6082  
(410) 837-5302

[dstanley@ubalt.edu](mailto:dstanley@ubalt.edu)  
[ctumosa@ubalt.edu](mailto:ctumosa@ubalt.edu)

Contact Phone Number

Contact E-Mail Address

  
Signature of President or Designee

**12.13.12**  
Date



The University of Baltimore proposes to offer this program at both the University of Baltimore campus and the Universities at Shady Grove (USG), with the exception of the Forensic Accounting specialization which will not initially be offered at USG. Additional information regarding the off-campus request is on Page 12 of this proposal.

## **Mission**

The mission of the University of Baltimore assures that the “university’s emphasis on career-oriented education attracts students with clear professional objectives and provides them with a broad foundation of knowledge to meet the rapidly changing conditions of today’s work environment as well as with the latest skills and techniques for productive careers in the public and private sectors.” Additionally, the University of Baltimore endeavors to “advance the intellectual, professional, and economic life of the metropolitan areas, the state of Maryland, the mid-Atlantic region, and beyond.” The mission of the University of Baltimore is comprised of four elements: (1) making excellence available to students motivated by professional advancement and civic awareness; (2) establishing a foundation for lifelong learning, personal development and social responsibility; (3) combining theory and practice to create meaningful, real-world solutions to 21st-century urban challenges; (4) and being an integral partner in the culture, commerce and future of Baltimore and the region. Within this broader context, the College of Public Affairs seeks to prepare problem-solvers who will analyze policy and lead public, nonprofit, health-care, and third sector organizations of the future.

The proposed inter-disciplinary M.S. degree program in Forensic Science – High Technology Crime (MSFS) will build on and support each of the institutional goals set forth by the University of Baltimore and the College of Public Affairs, while also contributing to the university’s projected growth goals. The interdisciplinary nature of the MSFS program may attract new students, interested in forensic science, health care fraud, and/or forensic accounting who might not otherwise pursue graduate study at the University of Baltimore. This will be accomplished by educating our MSFS students and meeting the need for experts in the rapidly changing field of high technology crimes; and by enabling our students to use the knowledge they have garnered for the successful investigation of crimes.

The MSFS will develop students’ knowledge and skills as experts in the recognition of high technology crimes, thereby preparing them to investigate the expanding area of criminal activity relating to technology. These high technology crimes include, but are not limited to, criminal activity involving the use of computer and digital information systems, accounting fraud, and health care fraud.

The University of Baltimore and the College of Public Affairs excel in the preparation and the delivery of education that has practical application (“Knowledge that works”). The goal has largely been to prepare students for opportunities at the local, regional and national levels. The School of Criminal Justice is uniquely situated to provide education to students who seek careers in forensic investigations, and the new degree program is a 21st century reflection of the university’s mission to impart knowledge that works and to provide students an opportunity to be agents of positive change.



## **Characteristics and Uniqueness of the Proposed Program**

### *Adequacy of Curriculum Design and Delivery to Related Learning Outcomes*

**Program Description:** The MSFS is designed to provide students with a broad based practical understanding of high technology crimes. The core of the program exposes students to forensic investigation techniques and skills, computer and digital information crimes, financial and health care fraud, prevention and security management strategies, and legal interventions and resolutions.

**Educational Objectives:** The graduate program in Forensic Science is designed to offer an opportunity for students who are interested in advanced forensic investigations of high technology crime relating to computer and digital information systems to develop advanced knowledge and skills that will allow them to compete for careers in government and private-sector corporations for highly evolving jobs in cyber security fields.

**Admissions Standards:** Acceptance into the MSFS is competitive. Applicants are expected to hold a bachelor's degree in a relevant field of study, with a minimum cumulative grade point average of 3.0, from a regionally accredited college or university. Students wishing to transfer from other graduate programs are expected to have maintained at least a B average in their prior coursework. Students whose GPA fails to meet the standards outlined above may be admitted to the program on a conditional basis, at the Program Director's discretion, provided that other aspects of the applicant's application reflect the ability to do satisfactory graduate level work in the program. Applicants should submit transcripts from all universities attended, a personal statement, and at least one letter of recommendation, in addition to a completed application for graduate study.

**Program Requirements:** Total number of credits – 42 Credits (13 Courses)<sup>1</sup>

The program requires the successful completion of 10 core courses and 3 courses in a specialization area. *More detailed course descriptions are attached.*

The proposed program will consist of core courses in forensic investigative techniques, cyber investigations, incident management, data protection, legal aspects of management, infrastructure protection, the globalization of crime, network security, fraud investigations, and data mining techniques. Presently, we are envisioning four specializations in the MSFS–High Technology Crime degree program: 1) Cyber Intelligence; 2) Forensic Accounting; 3) Health Care Fraud; and 4) Cryptanalysis. Students at USG enrolled in either the Cyber-Security BS degree or the BS in Criminal Justice and Criminology will have a clear pathway to advanced studies in their fields with the addition of UB's MSFS–High Technology Crime. The proposed program, with its applied pedagogy, features interactive learning not replicable in a virtual environment. Students already enrolled in programs at USG in science, nursing, business, and computer science, as well those in the undergraduate criminology and criminal justice programs may be interested in the professional pathways this program offers.

---

<sup>1</sup> The Forensic Accounting specialization will require an additional 3-credit course if the prerequisite requirement has not been met.

**CORE COURSES: 33 credits**

		Course Title	Hrs.	Status
1	FSCS 601	Legal Issues in High Tech Crimes	3	New
2	FSCS 610	Identifying Organizational Liabilities and Crime	3	New
3	FSCS 620	Forensic Investigative Techniques I	4	New
4	FSCS 720	Forensic Investigative Techniques II	4	New
5	FSCS 615	Information Retrieval	4	New
6	FSCS 724	Protection of Data/Information	3	New
7	FSCS 730	Incident Response I	3	New
8	FSCS 734	Incident Response II	3	New
9	FSCS 740	Internship	3	New
10	FSCS 750	Capstone (Project)	3	New

**Thesis/ Non-Thesis Option:** The final integrative component of the degree program is a core required Capstone Course. No thesis is required.

**FOUR SPECIALIZATIONS: 9 credits each****Cyber Intelligence**

#		Course Title	Hrs.	Status
1	FSCS 728	Information Systems, Threats, Attacks, & Defense Strategies	3	New
2	FSCS 727	Computer & Digital Forensics	3	New
3	FSCS 753	Computer & Digital Security Management	3	New

**Forensic Accounting (ACCT504 is a required prerequisite)**

#		Course Title	Hrs.	Status
1	ACCT 601	Forensic Accounting Principles	3	Existing
2	ACCT 603	Investigative Accounting and Fraud Examination	3	Existing
3	ACCT 604	Litigation Support	3	Existing

**Health Care Fraud**

#		Course Title	Hrs.	Status
1	HSMG 698	Health Care Fraud and Detection Analysis	3	New
2	HSMG 691	Health Planning and Evaluation	3	Existing
3	HSMG 702	Special Analysis and Health Care Fraud	3	New

**Cryptanalysis**

#		Course Title	Hrs.	Status
1	FSCS 630	Introduction to Cryptanalysis	3	New
2	FSCS 635	Image Analysis	3	New
3	FSCS 640	Steganography	3	New

		<b>Total Hours</b>	<b>42</b>	
--	--	--------------------	-----------	--



### *Adequacy of Provisions for Evaluation of Program*

**Student Learning Outcomes:** With the completion of the MSFS program, the student within their own specialization should be able to:

- Identify and articulate the many modes of attack through digital space on computer systems and how these relate to criminal acts
- Recognize the many modes of attack through digital space on computer systems and evaluate their relationship to criminal acts
- Develop specialized knowledge within their disciplines to remediate such attacks
- Evaluate commercial or governmental programs with regard to criminal attacks
- Design solutions for commercial or governmental programs with regard to criminal attacks
- Initiate and develop effective counter-crime management programs

**Course Evaluations and Assessment Plan:** Procedures for conducting program and individual course evaluations will be outlined in a program assessment plan to be developed for the MSFS prior to the implementation of the program. The plan will identify overall program learning objectives and measurable course level objectives for each of the required courses for the program. The plan will also outline a process for setting student learning goals and objectives. Annual assessments will be conducted, and the outcomes will be used to identify the strengths and weaknesses of the program to guide faculty in making improvements to the program and student learning outcomes. In addition to the internal program and course review process, an external program review will be conducted every seven years.

Student course evaluations, course syllabi, course materials, exams, assignment criteria, and classroom peer observation will be used to evaluate faculty.

### *Consistency with the State's minority student achievement goals and in the State Plan for Postsecondary Education*

The MSFS program is committed to minority student achievement and overall success. The program is in conformance with the University's long-standing commitment to the recruitment of a diverse student body. UB has proactively sought to identify multiple recruitment channels and communication strategies to ensure that there is outreach to a diverse population. The University also has a number of programs in place that will help the program's diverse student body persist until graduation. The University continuously assesses the success of these programs and has developed an achievement gap plan to further increase minority graduation rates of students.

### *Quantifiable & Reliable Evidence and Documentation of Market Supply & Demand in the Region and State*

The program, developed in consultation with the FBI, statewide law enforcement, and the chief executive officers at Citigroup Security, is intended for members of private corporations, nonprofit organizations, and governmental agencies who desire to advance their competencies in managing advanced technological resources to combat cyber threats, and related financial crime.

The most recent employment data (2010) from the Bureau of Labor Statistics affirms the demand for employees in cyber security related work, both within governments and in the public sector. The average salary for the greater Baltimore-Washington, DC- Northern VA areas, where statistics are taken, is over \$96,000. In Maryland, 68,000 people are employed in security related occupations and a recent search of Indeed.com, a jobs website, indicates 342 job openings at all levels in cybersecurity, with 307 at starting salaries of \$50,000 or more. Since 2010, the local presses have been reporting the increase in demand for qualified security personnel, revealing that private sector businesses in particular, are unable to hire "enough qualified workers" given "the tight pool of high-tech specialists and workers with government security clearances" ("Wanted Cybersecurity Pros" 1 August 2010 The Baltimore Sun). In addition, in February 2012, Sen. Barbara Mikulski presided at the opening of the new National Center for Excellence in Cybersecurity in Gaithersburg, MD with the purpose of encouraging partnerships between higher education, government, and private sector companies to educate students for evolving jobs in cyber security fields. Given the employment rates and the demand for new hires in this area, no one college, university, educational center or training program will be able to produce enough potential employees statewide. As noted in the February 2012 Southern Maryland Online article by Varun Saxena, "The creation of the National Cybersecurity Center of Excellence fulfills a goal identified in a 2010 strategic report on cybersecurity in Maryland" that emanated from the Governor's office. Within this same spirit, UMUC developed their program in cyber security at the undergraduate and graduate levels. A review of their course offerings suggests the focus of their program is in keeping with the 2006 National Science and Technology Council report, The Federal Plan for Cybersecurity and Information Assurance Research and Development. In contrast to programs focused on protecting information from unauthorized access, UB's program is centered around the "crime" that results from breaching information assurance protocols. UB's proposed program is interdisciplinary and focuses specifically on forensic cyber analysis.

### *Reasonableness of Program Duplication*

UB's proposed program is interdisciplinary and focuses specifically on forensic investigations of high technology crime. The program extends and complements our existing undergraduate degrees in Criminal Justice and in Forensic Studies, Health Systems Management, and Business.

The MSFS degree program is a uniquely defined area within the forensic discipline because of its emphasis on high technology crime, particularly that which occurs within the workplace. Currently, there are no forensic Masters' degree programs with an emphasis on High Technology Crime offered at any other USM institution, or any private or HBI institution within Maryland. There are two similar programs outside Maryland, one taught at the University of West Virginia and the other at George Washington University. Neither of these two programs impacts the catchment areas of the Baltimore region or Montgomery County.



## **Resources and Finance**

### *Adequacy of Program Faculty*

A combination of full-time faculty from the University of Baltimore and selected adjuncts from the commercial and government arenas with appropriate expertise and field experience will teach the courses.

The Forensic Program faculty are some of the finest professionals in the discipline, who have acquired decades of practical experience in the investigation and prosecution of crime. A complement of theoretical and practical expertise, forensic faculty work in metropolitan, state and national agencies, corporate and private industry, research with professionals from other countries and consult nationally and internationally. Many faculty are currently employed in law enforcement agencies, state's attorney's offices, forensic laboratories, and corporate and private security in the areas of fraud and high technology crime, with most serving in line and supervisory capacities. Qualified faculty include:

#### **Charles Tumosa, Ph.D.**

Professor Tumosa has close to a half century of experience as a Forensic Investigator. Charles Tumosa received his Ph.D. in Chemistry from Virginia Polytechnic Institute and State University in 1972. Dr. Tumosa retired from the Philadelphia Police Department's Criminalistics Laboratory in 1989 and the Smithsonian Institution in 2006. Dr. Tumosa has authored over 100 publications in forensic science, conservation science, chemistry, and numismatics. Currently, Dr. Tumosa is a clinical professor and the Forensic Laboratory Director at the University of Baltimore. He teaches the Forensic Investigations, Forensic Evidence, Incident Response, Trace Analysis, and various electives courses in the area of fraud including Forensics and Art, and Introduction to Questioned Documents. Dr. Tumosa has taught at the University of Baltimore since 2007.

#### **Ed Koch**

Edgar Koch received a Bachelor's of Science in Chemistry from Towson University and his Master's of Science in Criminal Justice from the University of Baltimore in 1988. He was the first forensic chemist in Anne Arundel County (AACo), where he established the Police Department's Crime Laboratory. Mr. Koch retired from AACo as Deputy Chief of Police in 1995. He subsequently became the Director of the Baltimore Police Department's Crime Laboratory, where he served for approximately twelve years. Currently, he is a lecturer in the Criminal Justice and Forensic Studies programs at the University of Baltimore. In addition to criminal justice courses, Mr. Koch teaches Forensic Science, Evidence Collection, Crime Scene Investigation, Forensic Investigations, Incident Response, and Microscopy. He has taught at the University of Baltimore for ten years.

#### **Berry Grant**

Berry Grant received both his BA in Jurisprudence and MBA from the University of Baltimore. He developed the first Criminal Intelligence and Computer Crimes Unit for the Baltimore City Police Department in 1993. He trained the Computer Forensic Examiners and managed the unit until his retirement. Upon retirement from the Police Department, he went to serve as the Senior Fraud Investigator with the Municipal



Employees Credit Union and a Background Investigator with Omniplex International Investigations. Mr. Grant served as the Chairperson of the Fraud Investigations Council for the Maryland-Washington, D.C. Credit Union League. Mr. Grant teaches a variety of police and forensic courses as well as the Cyberintelligence specialization courses.

#### **David Mabrey**

David Mabrey received his law degree from the University of Baltimore in 1990. He was admitted to Maryland Bar the same year. Currently, he is an Assistant State's Attorney for the District Court of Maryland for Baltimore City. In this capacity, Mr. Mabrey advises law enforcement on evidentiary issues, filing charges, and litigation procedures. He also trains new state's attorneys in case preparation, trial strategies and evidence review. Mr. Mabrey also served as an Assistant State's Attorney for the Circuit Court of Maryland for Baltimore City. In this position Mr. Mabrey tried homicide cases, fraud and identity theft crimes, developing legal strategies, consulting with medical examiners and conducting witness interviews. Mr. Mabrey has also served as a Faculty Advisor for Maryland State's Attorneys Association Trial Advocacy Program. He has taught at the University of Baltimore for approximately twelve years. In addition to law and criminal justice courses, Mr. Mabrey teaches Fourth Amendment Application and Interpretation and the Specialty Warrants, Wiretaps and Historical Conspiracies, Legal Issues in High Tech Crimes, and Organizational Liabilities and Crime for the Forensic program.

#### **John Pignataro**

John Pignataro has a Master's degree in Telecommunications and Computer Science from Polytechnic University. He is the Director of SIRT Investigations at Citigroup where he is responsible for all forensic investigations involving Computer and Digital Fraud for Citigroup in New York City. A former police Colonel for the Baltimore City Police Department, Deputy Superintendent for the Maryland State Police, and a Detective Sergeant for the New York City Police Department, Mr. Pignataro has more than 30 years' experience as an expert Computer Fraud Investigator. Mr. Pignataro can teach the Cyberintelligence and Cryptanalysis specialization courses.

#### **John Callahan, Ph.D.**

Professor Callahan has more than 25 years of public service with the federal government, his last assignment being that of assistant secretary of management and budget for the U.S. Department of Health and Human Services from 1995-2001. Professor Callahan can teach the Health Care Fraud courses.

#### **Phil Korb**

Professor Korb is the chair of the Department of Accounting and is a CPA. He has a research interest in income taxation of individuals and estates and trusts. He is the faculty adviser for the Theta Iota Chapter of Beta Alpha Psi. He has extensive research and referred publications in the accounting field. Professor Korb can staff the Forensic Accounting specialization courses.

#### *Adequacy of Library Resources*

The materials students need are largely available through open source databases, governmental archives, or online through organizations like the Department of Justice, Police Research Foundation, Westlaw, or a variety of professional organizations and

businesses. Peer reviewed material in journals is easily accessible through Langsdale Library's existing library subscriptions.

*Adequacy of physical facilities, infrastructure and instructional equipment*

Courses with a lab component will have classroom space that will allow students to break down computer hardware and hard-wire computer workstations and special software tools. Initially, the computer lab may be portable, however in the near future a designated "computer lab" space should be available on both campuses.

*Adequacy of Financial Resources*

Given the rich environment of high technology organizations in the Baltimore/Washington area, it is anticipated that the program will attract an initial class of sixteen students in its first year. We also anticipate that students will take at least three years to complete this program assuming that they take 15 credit hours per year. Data on anticipated Program Resources can be found in Table 1.

Data in Table 2 shows anticipated expenditures for the new program. We anticipate that as the program grows, additional faculty lines will be made available. In addition, we are providing for a one-course release for the program director. As noted in the program proposal, we do not anticipate that new resources will be needed from the library as many of the topical areas relevant to this area are available through ResearchPort. Staff assistance to faculty will be provided through the Academic Program Specialist assigned to the School of Criminal Justice. Student advising will be undertaken through the College of Public Affairs Advising staff. *No new resources are being requested.*



## M.S. of Science in Forensics Science

**TABLE 1: RESOURCES**

Resources Categories	Year 1	Year 2	Year 3	Year 4	Year 5
<b>1. Rallocated Funds<sup>1</sup></b>					
<b>2. Tuition/Fee Revenue (80% of (c+g) below)</b>	<b>137,856.00</b>	<b>189,552.00</b>	<b>241,248.00</b>	<b>292,944.00</b>	<b>344,640.00</b>
a. #F.T. Students					
b. Annual Tuition/Fee Rate					
c. Annual Full Time Revenue (a x b)					
d. # Part Time Students	16	22	28	34	40
e. Credit Hour Rate	\$718	\$718	\$718	\$718	\$718
f. Annual Credit Hours	15	15	15	15	15
g. Total Part Time Revenue (d x e x f)	172,320.00	236,940.00	301,560.00	366,180.00	430,800.00
<b>3. Grants, Contracts, &amp; Other External Sources</b>					
<b>4. Other Sources</b>					
<b>TOTAL (Add 2-4)</b>	<b>137,856.00</b>	<b>189,552.00</b>	<b>241,248.00</b>	<b>292,944.00</b>	<b>344,640.00</b>

<sup>1</sup> Revenue data is based on the assumption that the program will admit a specific number of students per semester (as shown above); and these students will take 15 credit hours per year and that most students will complete the program in three years.

**TABLE 2: EXPENDITURES**

<b>Expenditure Categories</b>	<b>Year 1</b>	<b>Year 2</b>	<b>Year 3</b>	<b>Year 4</b>	<b>Year 5</b>
<b>1. Total Faculty Expenses (b+c below)</b>	<b>89,253</b>	<b>89,253</b>	<b>133,880</b>	<b>178,506</b>	<b>178,506</b>
a. #FTE (Based on 382 Credit Hours per FTE)	1.0	1.0	1.5	2.0	2.0
b. Total Salary (based on 1 FTE faculty member \$70,000 ave.)	70,000	70,000	105,000	140,000	140,000
c. Total Benefits	19,253	19,253	28,880	38,506	38,506
<b>2. Total Administrative Staff Expenses (b+c below)</b>	<b>10,288</b>	<b>10,288</b>	<b>10,288</b>	<b>20,576</b>	<b>20,576</b>
a. #FTE	0.1	0.1	0.1	0.2	0.2
b. Total Salary (1 FTE=\$68,000 ave.)	6,800	6,800	6,800	13,600	13,600
c. Total Benefits	3,488	3,488	3,488	6,976	6,976
<b>3. Total Support Staff Expenses (b+c below)</b>	<b>5,767</b>	<b>5,767</b>	<b>5,767</b>	<b>11,534</b>	<b>11,534</b>
a. #FTE	0.1	0.1	0.1	0.2	0.2
b. Total Salary (1 FTE=\$40,000 ave.)	4,000	4,000	4,000	8,000	8,000
c. Total Benefits	1,767	1,767	1,767	3,534	3,534
<b>4. Equipment</b>					
<b>5. Library</b>					
<b>6. New or Renovated Space</b>					
<b>7. Other expenses (based on one trip at \$1,500, standard computer package, supplies, communications)</b>	<b>2,720</b>	<b>1,360</b>	<b>1,360</b>	<b>1,360</b>	<b>2,720</b>
<b>TOTAL (Add 1-7)</b>	<b>108,028</b>	<b>106,668</b>	<b>151,295</b>	<b>211,976</b>	<b>213,336</b>



### **Off-Campus Delivery of Program**

The program will be offered at both the University of Baltimore and the Universities at Shady Grove campuses. As noted above, there are no existing programs offering this degree program. The workforce demand for an increase in the number of hires in the area of computer and digital forensic investigators surpasses the current capacity of qualified workers. According to the newly formed National Cybersecurity Center of Excellence, "given the employment rates and the demand for new hires in this area, no one college, university, educational center or training program will be able to produce enough potential employees statewide." Offering the program at both campuses will provide an opportunity to potential students from two entirely different geographical locations within the State of Maryland.

The proposed program will consist of core courses in forensic investigative techniques, cyber investigations, incident management, data protection, legal aspects of management, infrastructure protection, the globalization of crime, network security, fraud investigations, and data mining techniques. Presently, we are envisioning three specializations in the Master of Science in Forensic Science–High Technology Crime (MSFS) degree program that may include computer forensic analysis, incident management, and cyber investigations. Students at USG enrolled in either the Cybersecurity BS degree or the BS in Criminal Justice and Criminology will have a clear pathway to advanced studies in their fields with the addition of UB's MS in Forensic Science-High Technology Crime. The proposed program, with its applied pedagogy, features interactive learning not replicable in a virtual environment. Students already enrolled in programs at USG in science, nursing, business, and computer science, as well those in the undergraduate criminology and criminal justice programs may be interested in the professional pathways this program offers. *The Forensic Accounting specialization will not initially be offered at USG.*

All courses will be taught in a classroom with a strong emphasis on interactive learning. A mix of both full and part-time on-site faculty from the Schools of Criminal Justice, Business, and Health and Human Services will deliver the program.

Academic Advisors from the College of Public Affairs and the Merrick School of Business will provide student support.

## **COURSE DESCRIPTIONS**

M.S. in Forensic Science – High Technology Crime  
University of Baltimore

### **Forensic Science Courses**

- FSCS 601      Legal Issues in High Technology Crimes      3 credits  
Examines the general regulations, general and computer-related law, and ethics and business policies associated with high technology crime. Areas of major focus include description of legal issues facing management and administration, traditional search and seizure as well as privacy issues, manager and supervisor responsibilities, criminal issues and definitions, chain of custody and ethical considerations. Problem-oriented course that focuses on applying the holdings of cases and analyses of statutes to different criminal fact patterns.
- FSCS 610      Identifying Organizational Liabilities & Crime      3 credits  
Defines problems, logic and theory, research protocols, personal and organizational risks, criminal and civil liabilities, physical security issues, due diligence matters, and environmental concerns and sexual harassment issues. Covers responsibilities of the organization and of the individual.  
*prerequisite: FSCS 601*
- FSCS 615      Information Retrieval: Paper and Electronic      4 credits  
Explores gathering of information and data, evidence collection, storage and security of records, personnel records and related issues, privacy issues, security of customer information, duties and obligations of the information technology field. Also focuses on legal access to these records.      *prerequisite: FSCS 601*
- FSCS 620      Forensic Investigative Techniques I      4 credits  
Focuses on traditional investigative techniques (interviews and interrogations), simple data collection, physical evidence, fraud detection, data acquisition and computer techniques, reverse engineering and industrial espionage. Also examines administrative process, the role of human resources and accounting, organizational processes and structures and chain of command/management. Intended as an introduction to FSCS 720.      *prerequisite: FSCS 601*
- FSCS 630      Introduction to Cryptanalysis      3 credits  
Provides the historical basis for ciphers and encryption techniques and examines the use of codes in government and commercial applications. Also explores decryption techniques as applied to businesses and to government.
- FSCS 635      Image Analysis      3 credits  
Examines the effective manipulation of digital images from digital photographs and videotapes. Discusses identification of authenticity and detection of manipulation in addition to detection of fraud and other criminal activity in these digital media.      *prerequisite: FSCS 630*



- FSCS 640      Steganography      3 credits  
 Steganography is a process by which information is hidden within other media. Presents tools (software) to detect such hidden information, including files, images, network traffic, disks, etc., that masquerade within any system. Also presents the processes of hiding or encrypting data to inhibit a forensic analysis and of the detection and counter-resolution of hidden information.  
*prerequisites: FSCS 630 and 635*
- FSCS 720      Forensic Investigative Techniques II      4 credits  
 A continuation of FSCS 620 with special attention on computer systems and network systems.    *prerequisite: FSCS 620*
- FSCS 724      Protection of Data/Information      3 credits  
 Examines prevention of data/information loss by theft, intrusion and natural disaster and assessment of vulnerabilities and their remediation. Also presents protocols for security and for effective data storage and examines assessment of risk.    *prerequisite: FSCS 615*
- FSCS 727      Computer and Digital Forensics      3 credits  
 Examines the use of specialized techniques for recovery, authentication and analysis of electronic data; reconstruction of computer usage; examination of residual data; and authentication of remaining data.    *prerequisite: FSCS 601*
- FSCS 728      Information Systems, Threats, Attacks and Defense Strategies      3 credits  
 Examines information systems and the threats from malicious activities that attempt to collect data from or disrupt, deny or destroy information within a system. Also explores origins of such attacks and effective responses to threats.  
*prerequisite: FSCS 615 and FSCS 727*
- FSCS 730      Incident Response I      3 credits  
 Explores the development of effective responses to active attacks on computer systems and networks, coupled with analysis of the breakdown of protective measures.    *prerequisite: FSCS 724*
- FSCS 734      Incident Response II      3 credits  
 Explores the management of emergency situations arising from natural disasters or civil disorder and the development of proper planning. Provides training in the proper maintenance of computer systems and networks that involve both the technical and physical security of systems, physical plant and personnel.  
*prerequisite: FSCS 734*
- FSCS 740      Internship      3 credits  
 Provides field experience to students through laboratory assignments with various forensic or criminal justice entities. Course is completed at the end of the program and requires submission of a journal and research paper. Eligible for continuing studies grade.    *prerequisites: Successful completion of all core courses in M.S. in Forensic Science program and permission of program director.*



- FSCS 750      Capstone Project      3 credits  
 Capstone course requires students to integrate and apply knowledge, theories, principles, skills and practical applications learned in FSCS core courses to actual high technology case scenarios. *prerequisites: Successful completion of all core courses in M.S. in Forensic Science program and permission of program director.*
- FSCS 753      Computer and Digital Security Management      3 credits  
 A study of the management of networks, types and sources of threats and vulnerabilities, risk management, firewalls and other security issues.  
*prerequisites: FSCS 615, 727, and 728*

### Accounting Courses

- ACCT 601      Forensic Accounting Principles      3 credits  
 Provides an overview of the field of forensic accounting focusing on the roles, responsibilities and requirements of a forensic accountant in both litigation and fraud engagements. Examines basic litigation and fraud examination theory, identifies financial fraud schemes, explores the legal framework for damages and fraud and damage assessments and methodologies, and reviews earning management and financial reporting fraud. Other topics include computer forensics and corporate governance and ethics. Actual litigation and fraud cases are used to highlight the evolving roles of forensic accounting.  
*prerequisite: ACCT 504 or equivalent*
- ACCT 603      Investigative Accounting and Fraud Examination      3 credits  
 Topics include the in-depth review of sophisticated fraud schemes, how fraudulent conduct can be deterred, how allegations of fraud should be investigated and resolved, the recovery of assets, methods of writing effective reports, and complying with SAS 82 and other fraud standards. Fraud and investigation topics cover acts of skimming, cash larceny, check tampering, register disbursement schemes, billing schemes, payroll and expense reimbursement schemes, improper accounting of inventory and other assets, corruption, bribery, conflicts of interest, security fraud, insurance fraud, anti-terrorist financing and money laundering. *prerequisite: ACCT 504 or equivalent*
- ACCT 604      Litigation Support      3 credits  
 Addresses the relationship between the forensic accounting professional and the litigation process in which he or she may play a role. Specifically, this course covers the litigation process, the legal framework for damages and fraud, damage assessment methodologies, issues related to the presentation of evidence through expert testimony, practices used in supporting divorce cases and basic rules of evidence as they apply to forensic accountants.  
*prerequisite: ACCT 504 or equivalent*



## **Health Management Courses**

- HSMG 698     Health Care Fraud and Detection Analysis     3 credits**  
Designed to familiarize students with the work of major federal health programs such as Medicare, Medicaid and the Children's Health Insurance Program. Identifies patterns of improper and fraudulent payments to providers in these programs, describes the forensic investigative techniques necessary to uncover fraudulent financial transactions such as payments, and examines the means to recover payments and to reduce future fraudulent practices.
- HSMG 691     Health Planning and Evaluation     3 credits**  
Explains the theoretical and historical foundations of health planning, the relationship between health planning and regulations, and the application of planning methods. Students gain an essential understanding of the basic structure and operations of health-care programs to determine the various points in the program at which fraud might occur.
- HSMG 702     Special Analysis and Health Care Fraud     3 credits**  
Provides a full understanding of major health-care fraud investigations conducted by the U.S. Department of Health and Human Services, Office of the Inspector General, and the U.S. Department of Justice Criminal Division. Students study the structure and operation of the Office of the Inspector General and its annual audit activities related to specific health-care programs as well as relevant reports issued by the General Accountability Office pertaining to health-care program improvements that could mitigate health-care fraud.