fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

News and Views

Issue Three FISSEA Year 2006-7 February 2007

IN THIS ISSUE

Letter from the FISSEA Executive Board Chair

Dear FISSEA,

This begins the end of our last *News&Views* newsletter for the current Executive Board's year. When I think of our ExBd, I can not help but compare it to the *X-Men* and *Wonder Women!* You know, the Super Humans who get the job done, no matter how great the challenge. Our Conference *Captain Marvel* is COL Curt Carver and *Captain America* is LTC Will Suchan, both from West Point. I frequently sing their praises for undertaking to pull together our most-excellent two-day two-track Conference. This year they were aided by *Boy Robins* Jim Litchko and Art Chantker as well as Jack Holleran. The *Wonder Women* included *Lois Lane*, LoC's MaryAnn Strawn providing advertising, and don't forget that *KungFu* begins with "K" and our own K Rudolph knocks out all competition when it comes to kreative genius. Our revamped Website was thanks to our *Spiderman* (get it?) NIST's Webmaster Patrick O'Reilly with support from *Super Girl* NIST's Peggy Himes and *Sheena* Susan Hansche. The contests were again purrfectly coordinated by *Cat Woman* Gretchen Morris. John Ippolito provided us with the wisdom of *Jedi Master Yoda*. *The Flash* was NIST's Mark Wilson who quickly solved challenges and raced back from vacationing in Sweden just to work on our Conference. The Extreme behavior of the ExBd is worthy of note. Cowabunga!.

Goings and comings occur in the best of teams and our *Justice League* was no different. *Alfred Pennyworth was the Butler who protected Bruce Wayne's mansion and Bat Cave,* and our *Alfreda* was NIST's Patrice Boulanger who accepted a promotion and left the Conference Registration work in the hands of *Batgirl* Kathy Kilmer and her NIST team. *Rocketman*, Charlie Farrell (from NASA) also moved into a different job and departed the ExBd.

So much for the fantasy hero metaphors… Here is a real Super Hero:

20 years ago, Rear Admiral Grace Hopper retired for the third time from the US Navy. She remains famous for discovering the first computer bug in 1951 and pasting the moth in her UNIVAC log book. I met her 30+ years ago and still carry the "nanosecond" she presented me as a memento. Her quotes are prognostic and numerous and the appropriate one for now is "In pioneer days they used oxen for heavy pulling, and when one ox couldn't budge a log, they didn't try to grow a larger ox. We shouldn't be trying for bigger computers, but for more systems of computers." In other words, lashing multiple small computers together instead of continually building bigger and bigger one. This relates to our ExBd. FISSEA is fortunate in not having just one executive to coordinate our activities but a group of actively participating volunteers to keep our beloved organization in top form, 20-years after its beginning.

Did you know that this is the year of the Spy, 2-"007"? It's been just under 20 years (18+) since *The Cuckoo's Egg* was published by Cliff Stoll. and we honor that landmark text by having an investigator who was mentioned in the Egg, Jim Christy, speak to our Conference. Spies are known for surreptitiously gathering whatever they need and another of our conference speakers, Todd Snapp, will wake us out of our complacency by explaining some of those

techniques and ways to teach our organizations how to protect against them. And, with ISSLOB moving from the fantasy world to reality, we plan to have the competition winners on the dais to answer attendee questions. For added insights on the future, our Keynoter, OMB's Karen Evans, will inform us of FISMA and other Federal initiatives. *News&Views* Editor, Nan Poulios, will put down her pen and speak about why Phishing is hard to prevent, and I will again have the honor of hosting the always intriguing Inspectors General panel. So, I hope that this will be a year when you can join your fellow members and attend FISSEA's 20th Annual Conference.

Stay Aware, Trained, and Educated with FISSEA,

Louis M Numkin, CISM
FISSEA Executive Board Chair

Pictured: Curt Carver (L) & Will Suchan, ensuring our 2006 Conference's quality.

Information Systems Security Line of Business (ISS LOB)

This message was forwarded by the FORUM of Computer Security Program Managers on behalf of DHS' Mike Smith on 6FEB2007.

"DHS, Office of Cyber Security & Telecommunications (CS&T) in coordination with the Office of Management and Budget (OMB), has announced the selection of six federal agencies as service providers to the federal government in the areas of information security awareness training and automated Federal Information Security Management Act (FISMA) reporting.

"Agencies selected to provide Security Awareness Training include the Office of Personnel Management, the Department of Defense, and the Department of State and the United States Agency for International Development who have partnered. Agencies selected to provide tools for automated FISMA reporting include the Environmental Protection Agency and the Department of Justice.

"These agencies will be the first to serve as Shared Service Centers (SSCs) for the new Information Systems Security Line of Business (ISS LOB). They have been selected through a competitive and analytically-derived process based on their qualifications to provide information security products and services on a government-wide basis. Each SSC is required to have a business process in place to support cross-agency servicing.

"SSCs will eliminate the need for each agency to develop security awareness training or obtain an automated tool for managing their FISMA reporting on their own. This will maximize resources and result in standardized information security programs and better-trained workforces, cognizant of their information security responsibilities. SSCs will also allow agencies to dedicate their limited resources to critical, mission-specific security issues.

"DHS, Office of Cyber Security & Telecommunications serves as the managing agency for the ISS LOB, part of the President's Management Agenda. By providing shared solutions for common information security areas, the ISS LOB will allow all Federal departments and agencies to benefit from improved levels of cyber security, reduced costs, elimination of duplicative efforts, and improved quality of service and expertise through specialization and consolidation.

"Through a phased approach, the ISS LOB will address a total of four information security areas that are common across the Federal government: Security Training, FISMA Reporting, Emerging Security Solutions for the Lifecycle, and Situational Awareness and Incident Response. Implementation of the first two security areas will begin in the third quarter of fiscal year 2007. .."

FISSEA Conference note: *Mike Smith will be presenting the ISS LOB Winner Panel at FISSEA's 20th Annual Conference so bring all you questions and get all the answers from the DHS/National Cyber Security Division ISS LOB - Program Management Office.*

Fool Me Twice

Todd Snapp
President, RocketReady

An ancient Chinese proverb says “Fool me once, shame on you; fool me twice, shame on me.” The fact is that, whether they are willing to admit it or not, people are gullible. No wonder businesses must now face the reality of hackers bringing age-old con artistry methods into the 21st century.

As organizations continue to wage war on computer hackers, the focus continues to be on technology defenses. Firewalls, access controls, intrusion detection, and secure communications are all essential components of a complete security barricade. But in recent years, an alarming number of security breaches have come through what some have dubbed the “human firewall,” more simply, the employees.

The practice of conning employees is certainly not a new one. The classic con artist, or "social engineer," hacks with a focus on employees rather than computers. As IT departments scramble to slam the gate on network infiltration, social engineers turn to infiltrating people. Social engineers have accomplished some of the largest security breaches and most vicious terrorist attacks in history. T-Mobile, Choicepoint, Visa, Hewlett-Packard, TJX and even the 9/11 attacks were all made possible by skilled human deception. Industry analysts such as the Gartner Group, say that it shows no signs of slowing either. They call it the “greatest security threat of the next decade.”

What better way is there to access sensitive information than with stolen credentials or information handed to you by an unsuspecting employee? What better way is there to view secured organizational information than to walk in the front door and open a file cabinet or sit down at an unlocked computer? What better way is there to learn the executive secrets of an organization than to “sit in” on their conference calls? There are no intrusion alarms, no suspicious activity, no denial of service just an “employee” accessing information made readily available to them.

Unfortunately, the job of thwarting would-be “human hackers” has often been a point of contention for IT security professionals as it falls in the gaps between multiple areas of responsibility. Should the CIO lead the charge? What about HR? Is it more an IT responsibility or facilities management responsibility? Is it really an IT security problem or more an administrative policy concern? These questions have seriously impeded the process of employee security. In many organizations the finger-pointing game has been further fueled by budgeting confusion and funding ends up being filtered into areas of security that are easier to categorize. As a result, social engineering, which is more difficult to define and classify, receives limited attention. All the better for social engineering hackers, who thrive on disorganization and slow office politics.

According to the Privacy Rights Clearinghouse, close to 75% of reported IT security breaches in the last year were accomplished with methods other than computer hacking. These breaches include all different types of fraud and theft that don’t require technical skills or a computer at all. Yet, in a society where people pride themselves on enlightenment and independence, few people will admit that they were a rube for con-artists. Fewer still know enough to recognize the creative techniques used by social engineers when they occur. Even so, most employees’ sense of security about business fraud causes them to think that they will know what to do when victimized. History shows that employees are an easily accessible sieve of information. Most often the breaches go unnoticed until private data gets in the open.

The effectiveness of social engineers can be tied to the skills and behaviors of the three main parties involved:

The Social Engineer: The social engineer is a clever and polished hacker who is quite aware of human tendencies. They select their targets carefully and strategize their attack so that their victim will often be apologetic that they could not provide more information. When performing their low-tech scam, the social engineer is careful to pace themselves and may even spend days or even weeks acquiring seemingly useless details which are building blocks for pursuing the items they are really after. In most cases, the building blocks are contact information, organizational structure, or internal terminology that will give them credibility when communicating with employees. The truly desirable items can be as simple as an employee ID or as damaging as private customer data or secure system passwords. The most significant factor in a social engineer’s behavior is their apathy toward their victim. Attacks are ruthless and can even include aggressive or intimidating methods. Regardless, the social engineer is well-prepared and is not concerned about defrauding or offending the victim.

The Victimized Employee: For most organizations, customer service is a top priority. Employees are encouraged to be accommodating and respectful to most anyone who needs their help. For the majority of employees, a call or message from a hacker is unexpected and peculiar, requiring the employee to make a quick decision and rely on instincts to prevent a security breach. For people in this situation, five factors slow their reaction time:

1. Reluctance to call another person a liar
2. Fear of personal consequences (loss of job or some reprimand)
3. Training to be helpful and never rude to a caller
4. Rationalization that the suspicious behavior is just a strange request by a legitimate person
5. Desire to avoid conflict or awkwardness

Desire to avoid conflict may be the greatest obstacle in defending against attacks. Many employees will often fulfill a suspicious request just to avoid tension. More damaging is the reluctance to report events once they have occurred. Rarely is a security breach prevented because of a pro-active report by an employee.

The Organization's Management: From a management perspective, a social engineering attack can be frustrating and difficult to identify. In particular, some IT security managers have struggled to develop defenses against an ever-changing threat to an ever-changing employee base. Since these attacks can result in long-lasting damage to the organization's reputation, managers are motivated to devise a response. However, procedural obstacles cause many executives to become cynical about the threat. Cynical reactions to employee security threats usually fall into six categories:

1. Social Engineering will eventually fade away like so many other methods of hacking.
2. Employees will always be the weakest link in security. There is nothing you can do to prevent employees from being duped.
3. IT Security Departments have enough to worry about without opening up the social engineering can of worms.
4. Definitions of social engineering are included in an organization's basic training program and this is all that is needed.
5. The organization is well aware of its points of weaknesses and will keep an eye out for issues.
6. Documented policies are clear about restricting the employee from giving out sensitive information and if they are followed there will be no problems.

These attitudes set the stage for public embarrassments where organizations are breached and IT security managers are the first on the chopping block. Progressive security managers identify the threat and develop creative solutions leveraging positive reinforcement and the employee's common knowledge of identity theft.

The combination of social engineering skill and employee kindness has made it so that even a poorly developed scam can have unprecedented success (case in point – the Nigerian Bank email scam). Social engineering threats merge security, organizational, and psychological weaknesses. In order to establish a successful shield against the onslaught of employee-targeted attacks, organizations must first take the threat seriously and then implement strong policy, training, and assessment tools. These will equip their human firewall to protect them from attacks and the employees themselves are the most powerful weapon of choice.

FISSEA Conference note: *This is a primer for Todd Snapp's eye-opening session on this topic during FISSEA's 20th Annual Conference.*

CompTIA RFID+

Tara Dean
Government Business Development Manager
CompTIA

Last month, FISSEA announced a pilot program in partnership with the Computing Technology Industry Association (CompTIA) that allowed FISSEA members to test out a new certification for professionals working with RFID technology. The certification, CompTIA RFID+, covers areas such as interrogation zone basics, testing and troubleshooting, standards and regulations, tag knowledge, design selection, installation, site analysis, RF physics and RFID peripherals, validating a technician's ability to install, maintain, repair, and troubleshoot the hardware and software functionality of RFID products.

The program provided 13 FISSEA respondents from 11 organizations in the retail, government, education and healthcare sectors with a voucher to sit for the exam in exchange for their feedback. The offer, which closed January 31, gives each participant an opportunity to evaluate an IT industry standard for the knowledge and skills required of workers who touch RFID and the sensitive information related to the technology. Participants have until mid-year to use their voucher and share their thoughts about the exam. As more agencies and organizations move toward adopting RFID technology to comply with mandates, this certification will become an important step in ensuring proper deployment and maintenance of RF systems, and feedback from FISSEA members will assist CompTIA in shaping exam content.

For more information on CompTIA RFID+ certification, please visit http://certification.comptia.org/rfid+ or email rfidplus@comptia.org.

FISSEA Executive Board 2006-2007

Louis Numkin, CISM, Board Chair**
louis.numkin@irs.gov
COL Curt Carver, Jr., Conference Program Chair**
curtis.carver@usma.edu
Art Chantker*
art@potomacforum.org
Susan Hansche, CISSP-ISSEP**
susan.hansche@nortelgov.com
John Ippolito**
jippolit@skipjack.bluecrab.org
James Litchko**
jim@litchko.com
Gretchen Ann Morris, CISSP*
gretchen.a.morris@grc.nasa.gov
Brenda Oldfield
Brenda.Oldfield@dhs.gov
K Rudolph, CISSP**
kaie@nativeintelligence.com
Mary Ann Strawn, Assistant Board Chair*
mast@loc.gov
COL Will Suchan, CISSP, Conference Director*
will.suchan@us.army.mil

Mark Wilson, CISSP, NIST Liaison
mark.wilson@nist.gov
Peggy Himes, Executive Assistant to Board
peggy.himes@nist.gov
Patrick O'Reilly, Webmaster
patrick.oreilly@nist.gov

* Term ends March 2008
** Term ends March 2007

FISSEA List Serve:

The NIST Computer Security Division is hosting the FISSEA membership e-mail list in support of FISSEA and the federal IT security community. The list is not moderated; any FISSEA member subscribed to the list can post a message directly to the list. This list will allow us to converse with other IT security professionals who have an interest in awareness, training, and education issues. Any issue related to federal IT security awareness, training, and education is fair game. It can be used to ask for help from the many veteran FISSEA members who have experience designing, developing, implementing, and maintaining awareness and training programs. Please refer to the FISSEA website for complete rules and guidance. To summarize the rules:

- No spam nor advertising unless it is for free training/workshops
- Respond to the sender rather than "reply to all"
- Avoid "me too" replies
- Do not send attachments

To post a message to the entire list, send it to fissea@nist.gov
If you want to be added or deleted send a message to fisseamembership@nist.gov

Federal Information Systems Security Educators' Association

Building better Computer Security through Awareness, Training, and Education

TRAINIA

This column's name is a contraction of the words "Training" and "Trivia." It includes information on upcoming conferences, book reviews, and even humor. The purpose is to provide readers with places to go and things to use in pursuing and/or providing Computer Security awareness, training, and education. However, FISSEA does not warrant nor determine the value of any inclusions. Readers are encouraged to do their own checking before utilizing any of this data. If readers have items to submit to this column, please forward them to Nan Poulios at nan.poulios@walshcollege.edu and Louis Numkin louis.numkin@irs.gov.

****

Payment of Expenses to Obtain Professional Credentials

OPM's Policy has the following in their Q&A guidance

"**Q: May the government pay for my licensing or certification examination?**

A: Yes. Your agency may pay for license and certification examinations as prescribed in title 5 CFR 5757."

The USC citation is quoted below as released 2005-05-26: U.S. Code, Title 5, Part III, Subpart D, Chapter 57, Subchapter IV, Section 5757, Payment of expenses to obtain professional credentials

(a) An agency may use appropriated funds or funds otherwise available to the agency to pay for --

(1) expenses for employees to obtain professional credentials, including expenses for professional accreditation, State-imposed and professional licenses, and professional certification; and

(2) examinations to obtain such credentials.

(b) The authority under subsection (a) may not be exercised on behalf of any employee occupying or seeking to qualify for appointment to any position that is excepted from the competitive service because of the confidential, policy-determining, policy-making, or policy-advocating character of the position."

****

FISSEA's own Jim Litchko has a new "free" service available to all. He will be sending out weekly thoughts titled: **THE I.C.E. GUY TIPS** to anyone who wants to protect their possessions and family and be prepared for emergency situation. If interested, contact Jim at: theiceguy@theiceguy.com

****

FISSEA's New Website

Our Webmaster, NIST's Patrick O'Reilly, has replaced our old website with the newly reconfigured version. Thanks, Pat, and contributing members of the FISSEA Exec Board for the volunteer effort. The location is still at: http://csrc.nist.gov/fissea

On your first visit, you may have to refresh your image (F5 key) if the old website initially displays on your screen. You can find up-to-date conference information, as well as our *News & Views* current and archived issues, and much more on the site. Please check it out and let us know what you think. Suggestions are always welcomed. Also, if any of your organizations have resources you wish to share, please consider submitting them for inclusion on the Resources page.

****

March 5-6, 2007. 6th Annual Mid-Atlantic Information Security Forum. Sheraton Premiere Hotel at Tysons Corner, Vienna, VA. Reserve your seat at the forum now and save! Full Forum Program $1350 Forum Faculty Dinner $ 85. Four ways to register: 1. WEB: http://www.regonline.com/DC07 2. PHONE: 617-399-8100 (weekdays 8:30 AM to 5:30 PM ET) 3. FAX: 617-399-8101 4. MAIL: Mid-Atlantic Information Security Forum, The Institute for Applied Network Security, 15 Court Square Suite 1100, Boston, MA 02108

****

March 7, 2007. Wireless Technology in Government Applications. Time: 2:00 PM Eastern / 11:00 AM Pacific.
Register today: http://www.1105info.com/zvbbvaw_hjwewa.html. Some Federal agencies have recently adopted wireless technology. From WWAN to WLAN (Wi-Fi) solutions, mobility and the ability to work anywhere has become of paramount importance. A broad range of applications - from intelligence gathering to housing and agricultural inspections to disaster relief efforts - all require real-time access to critical data. Additionally, new technological advancements offer significant improvements in information assurance, authentication paradigms, and long-term support. Participants will learn how wireless technology can improve the operational efficiencies of a Government organization with a foundation of information that could prove helpful when designing an effective end-to-end wireless solution.

****

March 9, 2007 - **Maryland Association for Higher Education (MAHE) Spring 2007 Conference** - Conference theme is "Safety & Security: Is your campus a disaster waiting to happen?" Panel and session topics include "Security Awareness, Training, and Education," "Designing Homeland Security and Information Assurance Curricula," "Disaster Recovery Planning," and more. For more information, please check out: http://www.bsos.umd.edu/mahe/

****

March 12-13 2007 – **FISSEA's 20th Annual Conference** –
Theme is "Looking Forward… Securing Today" Agenda, Location, Cost, and other information is available at http://csrc.nist.gov/organizations/fissea/2007-conference/ Y'all Come!

****

March 20-22, 2007 - This year **FOSE** will be held at the Washington, DC Convention Center. Registration is free for military, government, government contractors and educators, with valid ID, and $50 for business and industry. FOSE is only open to trade professionals. FOSE 2007 is proud to present the following keynote speakers: Mike Lazaridis, President and Co-CEO, Research In Motion (RIM); Gregory Q. Brown, President, Networks and Enterprise Executive Vice President, Motorola, Inc.; Michael W. Wynne, Secretary, United States Air Force; Paul Brinkley, Deputy Under Secretary for Defense, Business Transformation; Hector Ruiz, Chairman and Chief Executive Officer, Advanced Micro Devices
Register online at: https://www1.compusystems.com/servlet/AttendeeRegLoginServlet?evt_uid=325

****

March 30, 2007 - Capitol College is hosting its **22nd Annual Career Fair** for their students and others with engineering, computer science and technical skills - in the William G. McGowan Academic Center, on campus in Washington, DC. This is a FREE event for employers which provides a skirted table, two chairs, and Lunch. To register, go to: http://www.capitol-college.edu/administrativeoffices/careerservices/foremployers/careerfair.shtml and click on online registration. Phone questions to Tony Miller at: 1-888-522-7486 or e-mail careers@capitol-college.edu.

****

April 2-4, 2007 IMPACT 2007 "Building A Culture of Security". Fairview Park Marriott, Falls Church, VA
For Government and Industry Security Professionals. You are invited to attend a seminar that brings together the greatest single collection of expert speakers on DoD Security, Economic Espionage, Cyber Terrorism, Information Security, OPSEC, Personnel Security, Insider Threats, Security Clearances, Computer Security, JPAS, and the National Industrial Security Program. Organizer: National Security Institute. Platinum Sponsor: Pinkerton Government Services, Inc. Gold Sponsors: MathCraft, Inc. and The Centre for Counterintelligence and Security Studies. Benefits: Gain awareness and in-depth understanding of the security risks your company or agency is exposed to, and how to deploy the solutions that will safeguard your organization's critical information from terrorists, economic spies, foreign hackers and information thieves. Seminar admission includes pre-and post-conference JPAS workshops, continental breakfasts, luncheons, refreshment breaks, admission to Expo & Security Awareness Fair, and networking reception. The agenda is targeted to your needs. IMPACT 2007 is programmed by security professionals who are confronting the same issues, worrying the same worries and wrestling with the same problems. We organize the schedule to make effective use of your valuable – and limited – time by focusing on the issues you face both day-to-day and long-term. Register early and save $50. A special rate of $845 is being offered to all attendees whose registration and payment is received by March 1st. Register online today. Call the NSI Registration Team at (508) 533-9099. Complete conference agenda and session summaries are available at http://nsi.org/Impact2007/Impact2007.html

****

April 4, 2007 - **Engineering Malware** course via SANS@Home. The course runs for four sessions, and each session starts at 7:00PM and ends at 9:30PM, EDT. April 5th through April 26th. For complete course information and to register, visit https://www.sans.org/athome/details.php?nid=2646.

****

April 10-11, 2007 - MISTI is co-locating the **"Government Compliance and Cybersecurity Training Program**" with its two-day seminar on "Security Certification & Accreditation of Federal Information Systems" on **12-13APR2007** - at the Hilton Washington DC, located in Silver Spring, MD. Agenda may be found at:
http://www.misti.com/default.asp?Page=85&ProductID=6643&ISS=23177&SID=66_8571 and you can register at:
https://www.euromoneysecure.com/orders/MISTI/default.asp?abc=123&LS=&pag e=81&ProductID=6643

****

May 9-10, 2007 GovSec, U.S. Law and Ready! Conference and Exposition, Americas Premier Homeland Security Event, announced today that information technology (IT) security and government IT transformation will be major themes for this years conference and exhibition. Security is driving enterprise-wide transformation for federal, state and local governments as they clarify interoperability needs, intra-agency needs and intra-government needs. This transformation is driving the convergence of physical and IT security, which poses unique security interdependencies. The 2007 event, held May 9-10 at the Washington Convention Center, will include some of the foremost thought leaders in IT security and discuss the technologies needed to meet the needs of IT security experts, facility directors, law enforcement and first responders. Solutions to these IT and security challenges will be presented in the IT Security Hub on the show floor.

****

May 10, 2007 – FISSEA Free Workshop, "What's New in Security Awareness" at GovSec, 1:00pm - 2:45pm. Washington Convention Center is located at 801 Mount Vernon Place, NW, in Washington, DC.
Speakers: Susan Hansche, Louis Numkin, Jim Litchko. Join members of FISSEA to learn successful techniques and technologies to effectively increase employee and executive awareness of potential computer attacks. You will learn: When to use posters, presenters, promotions, PR and other communication tools; The latest tools to increase interactive, automated and Web-based awareness; Training and education strategies; and Resources for maintaining awareness. The Website with workshops is at: http://www.govsecinfo.com/hands_on_training_session.html
The Website for the Conference is at: http://www.govsecinfo.com/

****

May 23, 2007. 6th Free FISSEA Workshop, "Distance Learning: Making it Effective for Both Awareness and Training", 9:00am-12:00pm. to be held at the Library of Congress. See the flyer in the front of your conference handouts for complete details. Attendance is limited to 50. Pre-registration required by May 18. Please contact Susan Hansche (hansches@state.gov) to be a part of the panel or if there are any specific questions you would like to hear more about. Reservation contact Ashley Jones, jonesam2@state.gov or 703-204-6137.

****

HOMELAND SECURITY/IT ADJUNCT FACULTY POSITIONS Creative. Caring. Committed.
University of Maryland University College (UMUC) is seeking talented faculty to challenge students in one of higher education's most dynamic learning environments.
UMUC is hiring part-time adjunct and full-time non-tenure track faculty nationwide to teach Homeland Security/IT courses for on-site and online delivery formats. We invite you to learn more and APPLY ONLINE at:
http://clk.atdmt.com/BHD/go/fdrloumu0140000030bhd/direct/01/
We require a Terminal Degree (i.e., PhD, DBA, JD, etc) from a regionally accredited institution. However, exceptions may be made based on professional/industry and/or teaching experience based on specific academic discipline. Additional industry certifications may also be required for some academic disciplines.
As a UMUC adjunct faculty, you can share your knowledge and earn additional income while teaching within a flexible schedule that fits into your fulltime professional life. We provide online training for teaching with Webtycho, our state-of-the-art proprietary online platform.
UMUC is one of the 11 degree-granting institutions of the University System of Maryland. The university is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools. Today, we serve a diverse student body of over 90,000 students around the world.
OE/F/MC/V. Women and minority applicants are strongly encouraged to apply.