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

News and Views

Issue Two of FISSEA Year 2006-7 January 2007

IN THIS ISSUE

Letter from the Chair

We hope that you had a Happy and Healthy calendar transition. 2007 takes on added prominence as it marks the 20th Anniversary Conference for our organization.

If you have been a long term member, you know that we pride our organization on its camaraderie and the feeling of family. This is thanks to our friendly members and a sincerely helpful attitude and willingness to assist one another.

Should you be new to FISSEA, I hope you will make it to our Conference. Our Program Chair with the aid of the Executive Board is putting together a superb slate of informative presentations, spanning two tracks, along with notable quotable keynotes. You will walk away with much more than you had coming in, I assure you. More about the Conference is included within this newsletter edition.

It never ceases to amaze me at how fast we create new technologies and how fast many of them are compromised. MS Vista wasn't even out of the box when methods of how to breach it were demonstrated at a recent conference. For some of us, we never get to take the package off the shelf before it is already out of date and/or shot full of holes by viruses, hackers, etc. So, how can we help our employers and personnel do the right thing?

One way is to stay as current as possible on what is coming down the tech pipeline, especially as it might affect our organizations. The best way I have found is to subscribe to various related news services... and not just subscribe but actually review their content. Ensure that the data is from a reputable source, not just a front for marketing. But, should you get caught in the zero-day abyss of imminent technology change - where it is brought in too quickly, it's time to punt the query to a listserve such as ours in FISSEA. Ask your question and usually you will find another member who has either dealt with the situation, is going through it at the same time, or has some similar experience which may help you out.

I try not to forget the old testing problem: testers only tested whether a product did what it was supposed to do. Following early abuses we learned that testing must also include proving that the product did not do what it was not supposed to do. Today, the same is true of many applications and systems - their advertising touts how they do what they are supposed to do better than all competitors. But, until they are truly tested for failure points by those with no reason to polish the apple they are still only floating on a fantasy pond. It takes only one unknown hole to sink a ship.

Well, enough metaphors for this issue. The FISSEA Listserve is one thing which benefits our membership. Our website will become more informative as it gets restructured over the next few months. I would ask each of you who have specific suggestions for ways to make our organization and its tools more useful to please send them to me (remember, just me and not to the whole Listserve) so that we can consider them.

Only about a half of our members are currently on the e-mail list and therefore approved to use the closed Listserve. To get on the list, one can simply send an e-mail to fisseamembership@nist.gov , and our NIST support staff will make the Listserve available. Also, if you wish to be removed from the Listserve, please send a note to the same address, not the whole List. In closing, permit me to reiterate that guidance for the use of our tools is on our website, such as "Thou shalt send no advertising to the Listserve" and "Thou shalt not 'reply to all' when responding to a Listserve inquiry." Oh, and one more request... Please include "FISSEA" in the subject line for all communications.

Hoping to see you at our Conference. FISSEA will always be "Looking Forward ... Securing Today,"

Louis

2006-2007 Executive Board:

Col Curt Carver, Jr., Ph.D. ** *Program Chair*
U.S. Military Academy

Arthur Chantker *
Potomac Forum

Susan Hansche, CISSP-ISSEP **
Nortel / US Department of State

John Ippolito **
Allied Technology Group, Inc.

James Litchko **
Litchko and Associates, Inc.

Gretchen Ann Morris, CISSP *
RS Information Systems / NASA IT Security Awareness & Training Center

Louis Numkin, CISM **, *Executive Board Chair*
Internal Revenue Service

K Rudolph, CISSP **
Native Intelligence, Inc.

Mary Ann Strawn *, *Assistant Board Chair*
Library of Congress, Publicity

LTC Will Suchan, Ph.D., CISSP *, *Conference Director*
U.S. Military Academy

* Elected March 21, 2006 Term ends March 2008
** Elected March 23, 2005 Term ends March 2007

Mark Wilson, CISSP, NIST Liaison
National Institute of Standards and Technology

Peggy Himes, Executive Assistant of the Board
National Institute of Standards and Technology

Patrick O’Reilly, FISSEA (and CSRC) Webmaster
National Institute of Standards and Technology

Nanette Poulios, Newsletter Editor
Information Assurance Center, Walsh College

To view Executive Board bios and contact information, please visit the FISSEA website at http://csrc.nist.gov/fissea/ and click the Executive Board link.

Current Agenda for 2007 FISSEA Conference:

Please note, this agenda is a **current** schedule and is subject to change. Please visit the FISSEA website to get the most up to date agenda (http://csrc.nist.gov/). The agenda posted below was updated on January 18, 2007:

Legend
Admin or Break
Room One
Room Two

FISSEA 20: Looking Forward … Securing Today

Schedule (version 5)

12 March 2007		Time		13 March 2007	
Breakfast & Registration		7:30-8:15		Breakfast and Registration	
Welcome & Admin Notes	Will Suchan Curtis A. Carver United States Military Academy	8:15-8:30	8:15-8:20	Welcome & Admin Notes	Will Suchan Curtis A. Carver United States Military Academy
NIST Welcome	TBD NIST	8:30-8:45	8:20-8:45	Business Meeting	Louis Numkin, IRS Chair of FISSEA Executive Board
Keynote Presentations	Congressman Tom Davis (Invited) Congressional Cyber Security Challenge	8:45-9:15	8:45-9:45	Keynote Presentation	G. Mark Hardy, National Security Corporation
	Karen Evans, OMB (Invited) FISMA and Federal Initiatives	9:15-9:45			Chris Blask, Lofty Perch, Inc
Networking Break/Vendor Exhibits, Federal Business Council (FBC)		9:45-10:05*		Networking Break	
	"One Organization, Three Perspectives: Leadership, Security, Educator" Panel Organizer: TBD Pat Scarborough, Mike Smith, Brenda Oldfield DHS	10:05-11:05			Panel: Perils, Problems and Triumphs in Security eLearning Panel Organizer: Mary Ann Strawn, LOC Gretchen Morris, RSIS/NASA; Susan Hansche, Nortel/Dept of State; Terri Cinnamon, VA; Dr. Jim Chen, UMUC; Cheryl Seaman, NIH.
	NIST Standards and Guidance Mark Wilson, NIST	11:10-12:10			When Training Isn't the Answer: Electronic Performance Support Systems for Critical Information Assurance Audiences Jan Whiteley, National Reconnaissance Office
	Choosing and Using Proper Awareness Techniques John O'Leary, CSI				The Anatomy and Forensics of a Failed Course Al Payne & Jim Litchko
Lunch/Vendor Exhibits, FBC		12:15-1:15		Lunch/Speak Out	
	CIO Panel Challenges and Opportunities Panel Organizer: Jim Litchko, Litckho and Associates Jim Vanderhalf, Dept of State, TBD	1:20-2:10			Panel: IG Panel Panel Organizer: Louis Numkin, IRS IGs from NRC, Treasury, FDIC
	Change Management as it Applies to Awareness and Training Ellen Roth-Perreault, BAH				Why Phishing is Hard to Prevent Nanette Poulios, Walsh College
	DoD 85-70 Manual: Implication George Bieber, DIAP	2:10-2:40*			Hacking the Human Firewall Todd Snapp, Rocket Ready

	Information Systems Security Line of Business TBD				Computer Crime Jim Christy
Networking Break/Vendor Exhibits, FBC		2:40-3:00		Networking Break	
	Privacy Training – It’s All the Rage Donna Ebling, BAH	3:00-3:50			Networking & Information Security: Improving Online Learning Through Simulation Dr. Loyce Pailen & Julie Gilliam, UMUC
	Roadblocks in Developing New Security Professionals: Missing Foundations John Tesch, Colorado Technical University				Data Theft Michelle Barnum, Federal Government & System Integrators
Administrative Notes	Will Suchan & Curtis A. Carver United States Military Academy	3:50-4:00*	3:50-4:20*	Closing Ceremony Announcement of FISSEA Award Winners	Will Suchan & Curtis A. Carver United States Military Academy
Voting for Executive Board	Louis Numkin, IRS FISSEA Executive Board Chair	4:00-4:15	4:20-4:40	First Meeting, Executive Board	Louis Numkin, IRS
“Birds of a Feather” Gathering	TBD	4:15-6:00			
FISSEA Dinner at Local Eatery	Louis Numkin Cruise Director	6:00			

* = There will be door prize announcements throughout the day.
This is a preliminary schedule subject to change.

Congratulations to the 2006 Contest Winners!

Announcing Changes for 2007’s Contest

By Gretchen Ann Morris, CISSP
NASA IT Security Awareness and Training Center
FISSEA Executive Board Member

The annual conference has come and gone, and we announced our winners for the 2006 Trinket, Poster, and Website contest while we were there.

Congratulations again to our winners!

Trinket
K Rudolph, CISSP - Native Intelligence, Inc.

Poster
David Kurtz - U.S. Treasury Department, Bureau of the Public Debt

Web Site
Melissa Guenther, LLC, State of Arizona, Department of Economic Security

You can see the winning entries on the FISSEA web site.
http://csrc.nist.gov/fissea/

Due to feedback given in our conference evaluations, next year's contest will have a new name and two additional categories*.

New Name: FISSEA Security Awareness, Training, & Education Contest
Categories: Poster, Motivational Item (trinket), Website, *Newsletter, and *Interactive Scenario/Exercise

Keep your eye out for details as we get closer to March and the next FISSEA conference. Start thinking about what you may want to enter.

See you soon!
Gretchen Ann Morris, CISSP

FISSEA Security Awareness, Training & Education Contest for 2007

By Gretchen Ann Morris, CISSP
NASA IT Security Awareness and Training Center
FISSEA Executive Board Member

Showcase one or all of the following awareness, training, and/or education items you use as a part of your Security program. There will be one winner selected for each category listed below.

Awareness: there are four categories in this area:

- Poster
- Motivational Item (aka: trinkets - pens, stress relief items, t-shirts. etc.)
- Website
- Newsletter

Training & Education: there is one category for these areas:

- Interactive scenario/exercise

We will spotlight the winners with the FISSEA community! We also plan to share ALL entries with the FISSEA community. Below are the rules for the contest:

Rules and Guidelines

This contest includes five categories from one of FISSEA's three key areas of Awareness, Training, and Education. Each category of the competition will be judged separately. A winner will be selected from each category and awarded a certificate at the annual FISSEA conference.

1. RULES

a. Only one item in each category may be submitted (1 poster, 1 website, 1 trinket, I newsletter, and/or 1 interactive scenario/exercise). However, an individual or organization may enter in all five categories.

b. The entries must be submitted by a FISSEA member prior to the deadline of February 5, 2007.

c. Entries must have a security theme and be part of the organization's current security awareness, training and/or education program. All entries must be original and wholly unclassified.

d. A Contest Entry Form must accompany all entries and is available on the FISSEA website http://csrc.nist.gov/fissea. Each submission automatically agrees to allow FISSEA to publish.

e. PowerPoint will be used to prepare each entry. One slide will be designated the Entry Form for the category followed by the entry for that category. All slides should be e-mailed to: fissea-contest@nist.gov.

f. Any item not adhering to the rules and entry guidelines will be ineligible. The decision of the contest supervisor is final.

2. GUIDELINES

a. A committee of at least three FISSEA members will judge the contest. The judges will evaluate each category on the basis of originality, security message, and creativity.

b. The winners in each category will be announced at the FISSEA Conference. A certificate will be awarded to each winner with a congratulatory letter signed by the FISSEA Executive Board Chairperson.

Looking forward to seeing your entries!

Thanks!
Gretchen Ann Morris, CISSP

Free Awareness Posters

By Bill Uttenweiler, Business Manager
The Aerospace Corp., Cape Canaveral AFS, FL.

Our members and those of our local partners have created security education posters, and have been thoughtful enough to provide them in "soft" copy so that we can share them with everyone. They are in 8.5" x 11" PDF format. If you click on one of the images, your browser will open a new window and download the file from storage at our alternate web site *www.centralcoastsecurity.org*

You can then print one — or 100! The copyrights are retained by the various creators/contributors. We encourage your using them "as is" but you must get permission before making any modifications.

http://members.impulse.net/~sate/posters.html

Besides these, you should also skip down to our "seasonal" section. Previously published posters include themes include Valentines Day, African-American History Month, Easter, etc. It might be a good time to dust them off and use them again!

http://members.impulse.net/~sate/posters.html#Seasonal

We've had a dramatic drop in the numbers of new subscribers who sign up for these occasional e-mails. If you like the posters, please share the link with your colleagues.

Have a GREAT day, all! God Bless the USA!

Updating the “Human Firewall”

By Brendan Callahan
Director of Sales
RocketReady
Tampa, FL

Joan was going about her day as a help desk employee for a Fortune 100 financial services corporation when she received a call on her direct line. This was unusual, as most of her inbound calls come through the customer queue. The caller claimed to be a fellow employee, Dave White, from the IT Systems division in Dallas.

Joan: “Thank you for calling ______, Joan speaking. How may I help you?”

Dave: "Hi Joan, this is Dave White with IT Systems in Dallas. Don't worry, you're not in trouble. I just got an IOM from Craig Jones over here and we noticed some anomalies in how you log in. Are you logged in now?"

Joan: “Yes.”

Dave: “Good. Just go to your computer and - let's see – what log in are you using now?”

Joan: “Hold on a minute and I’ll check.”

Joan quickly went to work verifying Dave’s credentials. She looked up his name on the company intranet and found it listed under “IT Systems Dallas Office.” Also listed under that location, she saw the name, “Craig Jones.” She was confident that the person on the other end of the line was legitimate. After all, he called her direct line and his caller ID read “IT Systems Div” and showed the correct number. He even made reference to an “IOM,” or Inter-Office Memo – an acronym used every day in this company.

After a few minutes of friendly banter, “Dave” had Joan’s user name and password which allowed him to access the company’s customer database through the virtual private network that he established on his previous call, not coincidentally, with the real Dave White.

Although he seemed legitimate, “Dave” was a member of a team of ethical social engineers at a low-tech hacking and security training company hired by Joan’s company. Having worked at there for two years now, I’ve seen countless helpful employees get scammed even when following corporate policy. In this case, a few seemingly innocent calls to various departments in the organization yielded bits of information, like the acronym “IOM." These bits of information helped build the social engineer’s background story. To further establish credibility, the social engineer's caller ID was spoofed using an internet caller ID spoofing site to match the IT department’s location in Dallas.

What went wrong? Joan followed her company’s security policy to the letter, yet she fell prey to a social engineer and gave away her sensitive login credentials. In my experience, the attitude among many security executives is “people get fooled and there’s not much you can do to stop it.” This attitude has created a booming market for the makers of IT security applications and hardware, as security professionals focus on technical vulnerabilities.

Formalizing the ISSO Program: Creating a Cadre of Information Security Professionals At the Department of State

By Alison R. Guinasso
IRM/IA
U.S. Department of State

The Federal Information Security Management Act of 2002 (FISMA) requires all Federal agency heads to ensure that they have appropriately trained personnel sufficient to assist them in complying with Federally mandated IT security policies, procedures, standards and guidelines. The Department of State has the distinctive challenge of accomplishing this change at over 260 Diplomatic Missions overseas in addition to offices here in the United States. Each Foreign Service Post has unique information security requirements determined by the country in which it is located. This presents added demands on the personnel charged with the implementation of FISMA requirements.

The State Department’s Information Systems Security Officers (ISSO’s), both domestically and overseas, are the individuals primarily responsible for implementing all Department information systems security policies and guidelines and ensuring that the systems within their purview are configured and managed at acceptable levels of risk throughout their lifecycles. The State Department’s ISSO program is managed by the Enterprise Information Systems Security Management division under the auspices of the Chief Information Security Officer (CISO).

Currently, the Post Management Counselor or Bureau/Office Executive Director designates a person on his/her staff as the ISSO or alternate ISSO for each automated information system under their purview. In preparation for this assignment, appointees are provided with a 40-hour training course, Information Assurance for ISSO's. However, more than 89% of the Department's ISSO's perform this vital mission as a collateral duty.

In the past, the position of ISSO as a part-time function carried an acceptable level of risk. However, 9/11, the implementation of FISMA, along with the increased dependency on information systems, and the growing sophistication and escalating threat against the Department's key resources, convinced the Chief Information Officer (CIO), CISO and Office of Inspector General (OIG) that not only has this job increased to a full-time commitment, but more comprehensive training is required of ISSO's to properly execute their responsibilities.

In support of their decision, Richard McCormick, Information Systems Security Manager, IRM/IA, at the Department of State wrote a whitepaper entitled "Information Security Professionals & Formalizing the Information Systems Security Officer Program". Posted on the Office of Information Assurance's website in September 2005, this whitepaper builds a compelling business case for formalizing the ISSO program within the State Department. Most notably the document emphasizes the need for a professional training program plan to drive this process.

In taking a proactive stance on this issue, IRM/IA under the CISO has taken the following steps towards creating a formalized ISSO program:

Communications/Knowledge Sharing:
The Office of Information Assurance has implemented an ISSO List Service. This ISSO community tool allows for sharing information relevant to their responsibilities such as thumb drive usage, patch installation and recent threats to their systems. It has proven to be a unique resource for promulgating important information and informal guidance. In process is the development of a knowledge database which will house specific remediation solutions for specific threats that occur at Post.

Duties and Responsibilities:
The duties and responsibilities of the ISSO appear in more than ninety disparate Department of State policy citations with at least two different Bureaus creating permanent taskings for the Information Systems Security Officer. IRM/IA consolidated the duties and responsibilities into one document facilitating the ability of the ISSO to locate and understand a particular function. A portion of these duties were designed as a checklist and posted on the List Service so they could be used as a tool in the workplace.

Identifying and prioritizing their workload has always been a challenge to the ISSO. To this end IRM/IA has developed a draft 5FAM 1060 and 5FAH-11 that successfully brings together over seventy functions and will, once approved, provide a centralized point for editing current duties as technology and legislation change.

Training/Job Classification:
Currently the Department has role based training courses on Information Assurance for all employees from general systems users to non-IT managers to senior executives. As previously mentioned, ISSO's receive Information Assurance for ISSO's. However, as part of the plan to formalize this position, several agencies within the Department are collaborating to develop a detailed, comprehensive professional training program. This training program will be specifically designed to address the knowledge and skills required to perform their considerable duties and responsibilities.

ISSO of the Year Award:
The Department is in the process of implementing an ISSO of the Year award for an individual performing this responsibility at the highest level of achievement. This award brings attention to the importance of the ISSO in maintaining excellence in IT security at home and abroad.

The formalization of the ISSO program ultimately requires implementation of the official job and/or position description with an accompanying career track for this information systems security officer position. The CISO is promoting this key security role to a level of significance to encourage Information Technology personnel to pursue it as a career which will ultimately support the Department's global spotlight on security. By endorsing this process the Department of State is placing information security in the vanguard.

The Cyber Version of the "Dog Ate My Homework!"

By Derek E. Isaacs, Adjunct Professor
Computer Science/Security
Colorado Technical University Online

I had a student with an AiBo (Sony's electronic dog) that would download and vocalize e-mails and other documents. He had not turned in his last (200 point) Individual project - and received a 0. He called me up to plead his case and informed me that while processing his e-mail (along with his homework assignment) his AiBo 'shorted out - destroying (from the download) his assignment with no way to recreate unless he started from scratch. I politely asked him if I had his story straight – his electronic dog 'ate' his homework . . . after he said yes - I told him to redo the task - and come up with a better excuse next time.

TRAINIA

FISSEA Federal Information Systems Security Educators' Association
Building better Computer Security through Awareness, Training, and Education

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.

30JAN2007 will close Registration for this 1FEB2007 event:
A Note from NIST:
The first NIST Information Security Seminar for CIOs, CISOs, and IGs which was held on January 10, 2007 was very well received. However, numerous people had requested that their support contractors attend. To meet this need, we will hold the session again for all Federal employees and support contractor with information security responsibilities. This repeat performance will be held at NIST in Gaithersburg, Maryland on Thursday February 1st from 9:30 am - 12:30 pm. Registration is free, however all attendees must register in order to gain access to the NIST campus. Additionally, all support contractors must be sponsored by a Federal employee. The agenda, registration information, NIST campus access requirements, and directions to NIST are (available by contacting peggy.himes@nist.gov). Please note that the registration will close on Tuesday, January 30th at 12:00 p.m.

To learn more about this seminar, please visit http://csrc.nist.gov/sec-cert/ca-events.html

We look forward to another successful seminar,
William C. Barker, Chief
NIST ITL Computer Security Division

>>>>>>>>>>>>>>>>>>>>>>>>>>.>>>>>>>>>>>>>>>>

30JAN2007 - ISACA members e-Symposium on "COBIT: The Update" - earn 3 CPE Credits at no cost. Topics will include "An Introduction to COBIT 4.1 / Mapping COBIT to other Frameworks and Standards," "Implementing/Improving IT Governance using COBIT," "Conducting IT Assurance using COBIT," and "Current trends in IT Governance and Future Directions for COBIT."

To register, visit www.isaca.e-symposium.com.

>>>.

31JAN2007 will close this offer:
CompTIA is looking for 50 people who would be willing to take their new RFID+ Certification Exam. Participants are expected to already have experience and/or training,

as these free vouchers are for the test, alone. In exchange for the vouchers, CompTIA asks only that afterwards the test takers provide feedback on the exam. This offer is being extended to FISSEA though our members may not have direct knowledge of nor need for the certification. It is CompTIA's hope that our Awareness/Training/Education professionals may deal with staff who would benefit from being certified in RFID+.

If you or your staff are interested, please directly contact Ms Tara Dean by e-mailing TDean@CompTIA.org. Simply mention the FISSEA affiliation when speaking with her. Upon completion of the training please send me a note explaining your feelings on what was received and the overall process. Please note that this first-come-first-serve opportunity will close as of Wednesday, **31JAN2007**.

>>>.

31JAN-2FEB2007 - Society for Applied Learning Technology "New Learning Technologies conference" at the International Plaza Resort & Spa in Orlando, Florida - Bringing together senior professionals from government, industry, academia and the military to present the latest developments in the field of learning and training technologies. 82 speaker and four panel presentations. Case studies will be provided as well as the results of recent research on the effectiveness and utilization of the latest learning and training technology applications.

For more info, go to: http://www.salt.org/fl/orlando.asp?pn=orlando.

>>

31JAN2007 is the deadline for proposal submission(s) for MIS Training Institute's "IT Security World," – to be held in San Francisco at the San Francisco Fairmont Hotel, from **17-19SEP2007**. Presentation proposals must be submitted to proposals@misti.com by January 31, 2007. Four technical tracks and the following Sector Security Summits will be available: FinSec, HealthSec, RetailSec, GovernmentSec, EnergySec, and PharmaSec (new for 2007). All selected speakers receive: A complementary speaker registration to IT Security World 2007, Two half-priced registrations for colleagues or clients, and Exposure in the conference brochure and on the conference Web site. Real-world solutions to real-world problems where sessions are practical, objective and vendor neutral. Questions may be phoned to MISTI at (508) 879-7999 or e-mailed to mis@misti.com. More info available at http://www.misti.com

>>>

8FEB2007 - "Understanding the Lines of Business (LOB) Initiatives - Positioning Your Organization for Success" workshop - at the Willard Intercontinental Hotel in Washington, DC - Sponsored by Potomac Forum, Ltd. - Registration or Information at: www.potomacforum.org or Call: (703) 683-1613.

>>

For all of you *budding reporters*, FISSEA plans to publish another News and Views newsletter just before our 2007 Annual Conference so it can be printed and distributed to all attendees. If you have an article or TRAINIA item to submit, please do so by no later than 19FEB2007. That edition, along with all others, will reside in our website's archive, http://csrc.nist.gov/organizations/fissea/newsletters/ , for future historians to study. But, seriously, all appropriate submissions are solicited and welcomed. They will be vetted and edited, as necessary, and contributors will be celebrated into posterity. Sharpen your quill and start writing. Please send your text to our Editor: NPoulios@WalshCollege.edu

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

22-3FEB2007 - "Service Oriented Architecture in Government - What You Need to Know and Why - The Hype, the Truth, and its Role in Government" will be held at the Willard Intercontinental Hotel in Washington, DC – A Practical "Hands on" Workshop in an interactive classroom format for Civilian & DoD Government Agencies and Industry, transitioning to a Services Approach. Special Guest Speaker Kimberly T. Nelson, Executive Director for eGovernment at Microsoft Corporation, and the Former Assistant Administrator for Environmental Information & Chief Information Officer at EPA. Sponsored by Potomac Forum, Ltd.

Registration or Information at: www.potomacforum.org or Call: (703) 683-1613.

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>

26FEB-2MAR2007 - ISACA will hold its North America Training Week in Washington, DC at the The Madison Hotel 1177 Fifteenth Street Washington, DC. ISACA Training Week provides a unique educational experience. If you are an IS/IT audit, control or security professional in need of proven strategies and techniques for meeting the challenges you face every day, join your peers at our Training Week events.
Earn up to 38 CPE Credits. Register Online at:
http://www.isaca.org/Template.cfm?Section=Conferences&Template=/Conference/ConferenceDescByRegClass.cfm&ConferenceID=133

>>

5-6MAR2007 - 6th Annual Mid-Atlantic Information Security Forum – at the Sheraton Premiere Hotel in Tysons Corner ,Vienna, VA – More information is available by phone at : 617-399-8100, or. FAX: 617-399-8101.

>>

9MAR2007 - 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/

FISSEA 2007

March 12 & 13

Bethesda North Marriott Hotel
At White Flint Metro Stop

Looking Forward … Securing Today
20th Annual Conference

Learn new techniques and best practices

Stock up on ideas and resources

Great networking opportunities

First class learning, tremendous bargin price

http://www.nist.gov/public_affairs/confpage/070312.htm

Administrative/General Information: Peggy Himes, NIST
Phone: 301-975-2489; fax: 301-975-4964
peggy.himes@nist.gov

20-22MAR2007 – 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/industry. FOSE is only open to trade professionals. Go to: https://www1.compusystems.com/servlet/AttendeeRegLoginServlet?evt_uid=325

>>

30MAR2007 - 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.

>>

Beginning on **5APR2007** SANS is offering their "SANS Security 601, Reverse 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. For complete course information and to register, visit https://www.sans.org/athome/details.php?nid=2646.

>>

10-11APR2007 - 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=668571 and you can register at: https://www.euromoneysecure.com/orders/MISTI/default.asp?abc=123&LS=&page=81&ProductID=6643

>>

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 situations. To receive your copy, sign up at http://www.theiceguy.com/tips.html.

>>

Book Suggestions:
If you are a SCIFI aficionado you might be interested in reading The Daemon by Leinad Zeraus. This book describes some futuristic hacking by a legendary game designer. Of course we all know that a sophisticated game designer would never write and release such daemon programs. Food for thought from your FISSEA News &Views Editor.