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

News and Views

Winter Issue December 2008

IN THIS ISSUE

Letter from the FISSEA Executive Board Chair

Dear FISSEA Members,

Software vulnerabilities are up this year, especially Web browser-based ones, according to a new report from IBM Internet Security Systems. *The X-Force 2008 Mid-Year Trend Statistics Report*, released in late July, defined a vulnerability as anything that results in a weakening or breakdown of the confidentiality, integrity, or accessibility of the computing system. When a "hacking" story makes the front page, our leadership and co-workers take an interest in information assurance and IT security suddenly becomes the hot topic of interest across the mainstream—as happened when allegations emerged that China penetrated congressional computers back in June. Because of the "China incident", Bill S.3384 to amend section 11317 of Title 40, United States Code, to require greater accountability for cost overruns on Federal IT investment projects has gained bipartisan and leadership support from the Senate Homeland Security and Governmental Affairs Committee. Rumors have been circulated that this bill has the administration's support, which improves its chances of passing quickly. The Government Accountability Office (GAO) has stated that the legislation is a good idea because agencies need help. This bill's requirement to report cost and schedule breaches means that agencies will need to be more transparent with and accountable for poorly performing IT projects. As we approach the end of the 2008 Federal Information Security Management Act (FISMA) reporting period, I would like to share information resources that could help keep your agency off the front page and raise your FISMA reporting stats for 2009.

That said, the Defense Information Systems Agency (DISA) mission is to plan, engineer, acquire, field, and support the command, control, communications, and information systems needs of the Department of Defense (DoD) in times of both war and peace. One vital aspect of the DISA mission is much like FISSEA--to provide valuable, timely and accurate education, training, and awareness to the DoD components.

DISA's Field Security Operations (FSO) branch provides IA training products to the DoD and the non-DoD community in support of their mission. DISA's training products consist of Web-based training (WBT), computer-based training (CBT), and VHS videos. Many of these are offered and shipped to customers free of charge. One product offering is Critical Infrastructure Protection (CIP). The CIP WBT provides baseline CIP awareness to enhance the knowledge of personnel in the front lines of defense, DoD and other government CIP planners, infrastructure owners, managers, technicians, and users. CIP-WBT provides an overview of the systems that comprise the critical infrastructure, what CIP is, the national organizational structure of CIP, how DoD fits into the national CIP organization, and DoD CIP organizational structure and responsibilities. The course goes into detail on the DoD infrastructure sectors and special function components and concludes with the six phases of the CIP lifecycle.

The System Security Authorization Agreement (SSAA) Preparation Guide contains guidance on completion of the SSAA while accomplishing the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). After presenting an overview of the DITSCAP, this Web-based product provides

detailed guidance on the contents necessary to complete a SSAA using the outline presented in the DoD 8510.1–M, *DITSCAP Application Manual*. The target audience for this product is information system certification team members, information assurance managers (IAMs), information assurance officers (IAOs), system administrators (SAs), and personnel responsible for writing, processing, or reviewing SSAAs. This product is also useful for preparation of a SSAA using the National Information Assurance Certification and Accreditation Process (NIACAP), in the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000.

Among the Web-based training products is Information Assurance Policy and Technology (IAP&T) the replacement for Operational Information Systems Security (OISS) CD–ROM. The IAP&T training courseware has been created for users performing duties as IAMs, IAOs, or SAs in accordance with DoD guidance (DoDD 8500.1 and DoDI 8500.2) pertaining to the defense of information systems. Individuals assigned to duties involved with policy and oversight, inspection and audit, or other functions supporting the IA mission (e.g., prevention, detection, and eradication of viruses; execution and evaluation of system audit records; access control; disposition of Information Systems (IS) media; and development and compliance with the risk managed approval of system operation [certification and accreditation] plans) will find this course useful and meaningful. Depending on the Command, Service, or Agency (C/S/A), the completion of this online course could help students meet the DoD and C/S/A standards for Level 1 System Administrator certification. For more on the training mentioned, visit http://iase.disa.mil/eta.

System downtime caused by software vulnerabilities is expected to triple in 2008 if you don't take proactive security steps. The Transportation Security Administration (TSA) was one of the more recent agencies to learn firsthand about the challenge of protecting personal data stored on a mobile computing device. Misplacing a laptop containing un-protected personal data highlights data security vulnerabilities within the federal government; despite a two-year effort to improve security. Keeping these "stories" from occurring in the first place is often a matter of following rudimentary procedures. In fact, I have read that routine practices can prevent more than 90 percent of hack attempts. That said I hope this information will help prevent your agency from becoming the target of a hacker or the topic in the morning news.

Emma A Hochgesang-Noffsinger
FISSEA Executive Board Chair

Environmental Changes

Emma A. Hochgesang-Noffsinger

With the impending change in administration and the numerous political advertisements focusing on a variety of topics, my thoughts continue to wander to our environment. My focus is not necessarily on global warming, but leaning more toward our communication environment. Wikis, widgets, blogs, blogging, news feeds, podcasts, or social networking to reach out and communicate with colleagues, teleworkers, others in our profession and the public. Approximately 90% of my organization (Headquarters Air Force, Information Management Resource Division) is participating in a telework pilot program, using flexiplace or flexible work hours, and (or) works a compressed work schedule (working 9 hour days, with 1 day off every other week). These flexible work options make work more enjoyable because they promote a balance in our work and personal lives. I will attest -- it has been an absolutely wonderful experience. In addition to revitalized attitudes, there is a "new" tone in conversations around the water cooler and coffee pot that indicate a renewed dedication and loyalty toward our organization. Among other "firsts" my revitalized telecommuting co-workers and I have been experimenting with podcasts and taking advantage of the benefits of audio teleconference, web conference, and other collaborative capabilities. These tools have resulted in increased productivity, agency cost savings, and other benefits for all employees, particularly the teleworkers.

What has any of this to do with FISSEA? In the coming year, NIST will explore offering this type of capability to our FISSEA web site! How cool is that? "Wiki" technology could be available in 2009. Not to get your hopes up only to dash them, the final decision will likely be dependent upon budget. As with most agencies, technology is affected by the availability of funds, so I cannot promise availability, just the possibility. I will keep you informed of any decisions and of course the best information source is the FISSEA web site, FISSEA newsletter, and my email updates. If you are not receiving these updates regularly, verify that we have your correct email address by sending your contact information to: fisseamembership@nist.gov

As I sit and glance around, I appreciate that I am able to write this article from my home office as today is a telework day.

FISSEA 10th FREE Workshop

Susan Hansche, CISSP

On Thursday, November 13th, FISSEA hosted our 10th FREE workshop: Information Systems Security Qualifications Matrix: Complexities, Competencies, Experience, and Training. FISSEA is proud to have worked together with the CIO Council IT Workforce Subcommittee to organize this successful event for our FISSEA members. The Information Systems Security Qualifications Matrix is a CIO Council initiative to establish qualification levels for staff engaged in Information Systems Security work. The matrix is designed to ensure general consistency across the Federal government. The matrix, currently under development, will describe the competencies; suggested experience; and suggested education, training and development needed for successful performance of assignments by individuals (federal employee and may be used for contractors) responsible for federal information security.

Workshop participants (both those in attendance and those who dialed-in) worked on two activities to help define the attributes for the matrix. The first small group activity involved a review of suggested requirements expected of Information System Security Professionals in their organization, including the potential qualifications criteria (proficiency levels, competencies, education, training and career development, and certifications). The second activity focused on prioritizing a given set of information system security roles. Both of these activity worksheets and the PowerPoint presentation are available on the FISSEA website under workshops. The executive board encourages all FISSEA members to review the documents and submit comments directly to Dagne Fulcher, who is leading the matrix development for the CIO Council IT Workforce subcommittee.

Finally, we would like to thank the CIO Council for providing a toll-free dial-in number for the workshop and a special thank you to Captain Cheryl Seaman, Office of the Chief Information Officer, at the National Institutes of Health, for offering the beautiful and convenient Natcher Conference Center in Bethesda, MD for the event.

FISSEA Supports FIAC 2008

Louis Numkin, CISM

The Federal Information Assurance Conference (FIAC) 2008 is in the history books. FISSEA hosted a thread of four sessions which seemed to go well with our audience. Executive Board members Mark Wilson, Susan Hansche, Loyce Pailen, and Louis Numkin provided sessions and introduced Keynote speaker Mischel Kwon, the new Chief of CERT. Lakshmi Narasimhan and Jim Litchko worked in the FISSEA exhibit booth, passing out fliers for our 2009 Conference and November Workshop, as well as signing up new FISSEA members.

The Ronald Reagan Building was a beautiful huge venue, the food was plentiful and delicious, and the end-of-day social was pleasant and great for networking. Registered were 308 attendees with 46 vendors and exhibitors displaying their wares. FISSEA lends support to several conferences each year - the next one on our calendar is GovSec - and FISSEA assists agencies to develop upcoming Cyber Security Days with recommendations and speakers.

FISSEA Educator of the Year Award

If you work with someone (or know someone) whose outstanding work during 2008 in information security awareness, awareness training, role-based training, education, or certification (of people) is deserving of “public” acknowledgment and appreciation, this is an opportunity you don’t want to miss! Submissions are now being accepted for the FISSEA 2008 Educator of the Year Award which will be presented during our 2009 Conference. Submissions will be accepted through Tuesday, February 12, 2009. For details, please visit the FISSEA Educator of the Year page on our website.

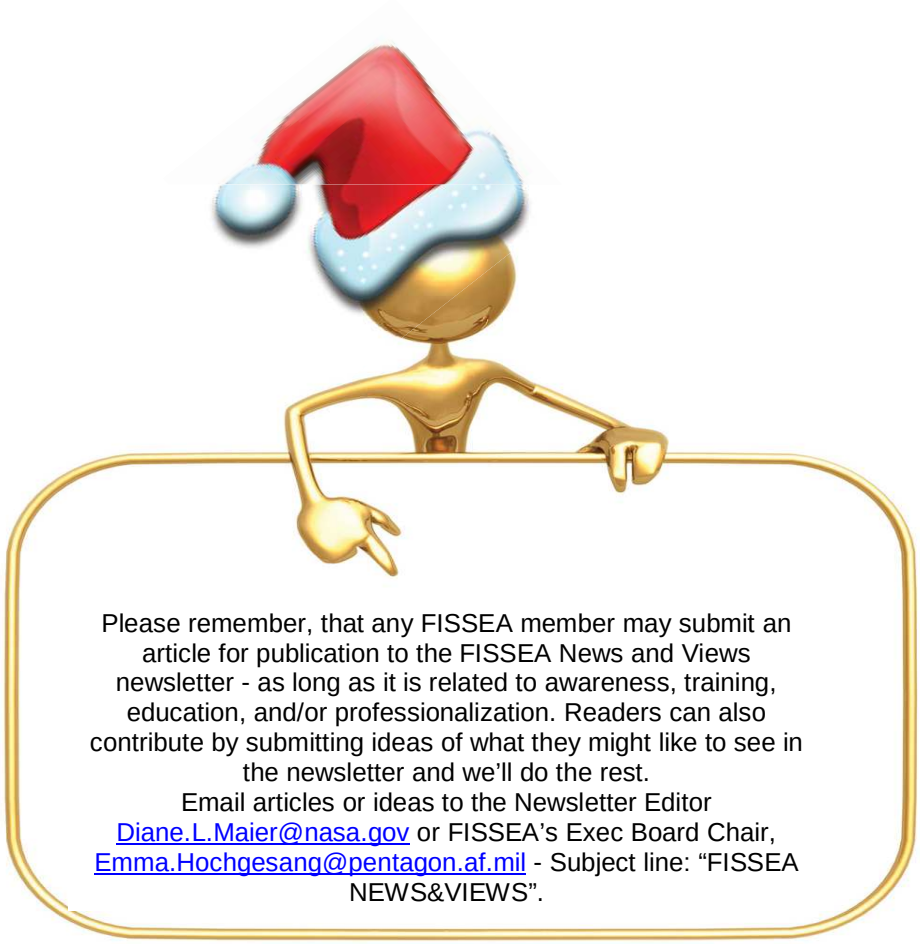
FISSEA Executive Board Members Term 2007-2009	FISSEA Executive Board Members Term 2008-2010
Susan Hansche Nortel/U.S. Department of State Workshop Coordinator susan.hansche@nortelgov.com	**Emma Hochgesang-Noffsinger** HQ Air Force, CIO Support Directorate FISSEA Executive Board Chair emma.hochgesang@pentagon.af.mil
John Ippolito Allied Technology Group, Inc. ippolitoj@hq.alliedtech.com	**Maria Jones** US Department of Labor OSHA FISSEA Assistant Board Chair jones.maria@dol.gov
Louis Numkin Retired IRS FISSEA Conference Director 2009 lmn@juno.com	**Richard Kurak** NASA IT Richard.s.kurak@nasa.gov
Loyce Best Pailen University of Maryland University College lpailen@umuc.edu	**Gretchen Morris** DB Consulting Group/NASA ITSATC Gretchen.A.Morris@nasa.gov
Mark Wilson NIST mark.wilson@nist.gov	**Lakshmi Narasimhan** East Carolina University narasimhanl@ecu.edu
	Cheryl Seaman National Institutes of Health FISSEA Conference Program Chair 2009 seamanc@mail.nih.gov
Other FISSEA Contacts:	
Peggy Himes NIST NIST/FISSEA Co-liaison peggy.himes@nist.gov	**Diane Maier** DB Consulting Group/NASA FISSEA Newsletter Editor diane.l.maier@nasa.gov

FISSEA List Serve:

The NIST Computer Security Division is hosts 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 users to converse with other IT security professionals who have an interest in awareness, training, and education issues. Any issue related to FISSEA's mission, 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, but to summarize the rules:

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

Abuse of the list guidelines will lead to removal of the abuser's access.
To post a message to the entire list, send it to fissea@nist.gov
If one wants to be added to or deleted from the list, send the request to fisseamembership@nist.gov
This address should also be used if one wishes help in determining whether an item is list appropriate or not.



Please remember, that any FISSEA member may submit an article for publication to the FISSEA News and Views newsletter - as long as it is related to awareness, training, education, and/or professionalization. Readers can also contribute by submitting ideas of what they might like to see in the newsletter and we'll do the rest.
Email articles or ideas to the Newsletter Editor Diane.L.Maier@nasa.gov or FISSEA's Exec Board Chair, Emma.Hochgesang@pentagon.af.mil - Subject line: "FISSEA NEWS&VIEWS".

Federal Information Systems Security Educators' Association

Building better Computer Security through Awareness, Training, and Education

-Artwork by K. Rudolph, John Orban, and Louis Numkin.

TRAINIA

This FISSEA News&Views Newsletter column's name is a contraction of the words "Training" and "Trivia." It usually 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 Louis Numkin at LMN@JUNO.COM and Diane Maier Diane.L.Maier@NASA.Gov . Please place "FISSEA Trainia Submission" in the Subject line.

****

FISSEA's 22nd Annual Conference

FISSEA's 2009 Annual Conference, *Awareness, Training and Education: The Catalyst for Organizational Change* will again be held at The National Institute of Standards and Technology (NIST) in Gaithersburg, MD, Tuesday through Thursday, **March 24, 25, 26, 2009**. Information systems security professionals from Government/Industry/Academia who are trainers, developers, educators, managers, CIOs, CISOs, and researchers involved with information systems security Awareness, Training, Education, Certification and Professionalization should attend.

Please mark your calendar now and we will fill in the blanks via website postings and e-mails as we progress through our planning process. If you have any questions relating to our 2009 Conference, please address them to Louis Numkin LMN@JUNO.COM, Conference Director, or Captain Cheryl Seaman seamanc@mail.nih.gov , Program Chair.

****

Virus Alert

Another e-mail Virus alert is making the rounds. Just in time for Christmas mailings, there is a new virus circulating in the UPS delivery system. It applies to Fed Ex as well. You will receive an e-mail from UPS Packet Service along with a packet number.

Note that the word packet is misspelled on this line (paket).It will say that they were unable to deliver a package sent to you on such and such a date. It then asks you to print out the invoice copy attached. DO NOT TRY TO PRINT THIS! IT LAUNCHES THE VIRUS!

Snopes confirmation is at: http://www.snopes.com/computer/virus/ups.asp

****

Educational Opportunities

ISACA wants to let you know that it has numerous educational opportunities coming up. Here are a few:

FEBRUARY

23 – 24 Computer Audit, Control and Security (CACS) Conference, Kyoto, Japan

MARCH

2 – 6 ISACA Training Week, Houston, TX
15 – 18 EuroCACS (Computer Audit, control and Security), Frankfurt, Germany

For more info on ISACA's offerings, visit the ISACA web site at: http://www.isaca.org.

Ziff Davis Enterprises has e-seminars open to all interested in their subjects. There most recent, as of this writing, dealt with Virtualization for Business-Critical SAP on SQL Serve r. Prior to that were subjects like: creating an effective SOA Quality Management Strategy with Web 2.0; Real Time Connections – Real World Threats; and the New Age of Video Surveillance. These were aired in September but if you missed them, they can be rebroadcast on demand, just e-mail eSeminars@ziffdavisenterprise.com

PCMagCast Learning Center has a free course you may want to check out. Small businesses are making much more use of wireless hotspots, mobile devices and wireless services, but, in many cases, their wireless usage creates increased security threats. Unless users take the proper steps to secure their devices and their wireless sessions, they can expose key business data to others, and allow unwanted access to business networks. It's also easy for them to invite these threats if they don't have proper security set up on their home wireless networks.

Simple steps such as running firewall software and wireless security suites can help protect private business information. In this free online PCMagCast Learning Center course, you learn what you need to know about setting up a secure wireless network, secure usage of wireless hotspots (Public WiFi), and how to deploy security software to keep you safe and prevent unauthorized access.

More information and online registration may be found at:
http://ct2.eletters.whatsnewnow.com/rd/cts?d=42-1785-1-464-1093729-507649-0-0-0-1-3-118

****

In-SITE-ful Info:

News on 12SEP2008: "If the Federalist Papers were written today, it would have been against Virgina's Anti-SPAM Law to use the Internet to distribute them." Therefore, Virginia's Supreme Court struck down the state's Anti-SPAM Law. Individuals should not use networks to send out unsolicited e-mail but the Court determined that this State law was contrary to the Second Amendment of the US Constitution. Civil Libertarians applauded the ruling but the case may now go to the Supreme Court of the United States.

On **Kim Komando's radio show** 13SEP2008, it was stated that Firefox will keep your passwords in a protected file. Furthermore, it will remember where they go so you don't have to enter them. However, you have to remember the password to the protected file. If you forget it, you'll have to crack it. Remembering the password is a lot easier! The procedure if you want Firefox to remember your passwords, is to click Tools>>Options. Click Security. Check the box next to "Remember passwords for sites." Also, check the box next to "Use a master password." Enter your master password twice. Click OK. Thereafter, when you are surfing and come upon a site that requires your password, Firefox asks for your master password. You enter it. The password for the site will be provided.

Cell Phone Security Myth and Facts: Tests have been run and the Internet warnings about cell phones having strong enough radiation to pop popcorn kernels have been adjudged a myth. Of course, the more serious reports of concerns over the long term effects of heavy cell and cordless phone use on human tissue are based on fact and a real health concern. One more cell fact is that Kiplinger has reported that "Claiming cell phones as a tax free fringe benefit will get easier soon: Congress is prodding IRS to loosen rules that require taxing personal use of employer-provided cell phones and keeping detailed records of business usage. Under current IRS rules, workers have to document the business purpose, time and place of calls they make. Lawmakers say cell phone usage should be on a par with employee use of company desk phones or e-mail, which needn't be tracked."

Security Movie Review

Have you ever found someone's disk and wondered what it might be worth? The recent Conn Brothers movie, "Burn After Reading," deals with a couple gym employees (McDormand and Pitt) who come up with a disk of SECRET information which they try to sell for big buck$. Other notable actors include John Malkovich and the critique I've read says that the flick has at least two really good funny scenes.

Check It Out

- BLACKLE is an energy saver for your Internet searches. In a sense it is a black screen Google where gray letters are displayed on a black background. This actually saves energy and Google quotes a blog estimate that "using Blackle could save 750 megawatt hours a year" but even if it didn't, it would remind users to conserve energy.

- For those of you that like storms, http://www.Stormpulse.com is the perfect place to go to learn where any storm is heading within the USA. It provides lots of info on conditions, photos, power, approaches to major cities, etc. There is also an archive for researchers and students. This should be useful info for those involved in DR and CP for organizations.

- *Create a Sustainable Compliance Program* is a white paper which examines trends in compliance and security management and approaches to reducing the cost and operational burden of compliance in the future. It examines how to create scalability in your compliance efforts and illustrates how to automate your compliance efforts with scalable processes to reduce manual compliance and gain efficiencies for future efforts. Download at: http://www.netiq.com/go/Compliance_wp/?origin=NS_ISACAJO_090108

Extras...

The CSO Security Leader from 15SEP2008 included a few interesting reads:

1. Security ROI: Fact or Fiction? Bruce Schneier takes issue with the terminology and with vendor-created "ROI calculators". See: http://cxolyris.cxomedia.com/t/2588861/1414060/28438/0/
2. Security Awareness Training, With Style. Perimeter eSecurity's Jason Miceli shows how to create high-impact security awareness messages. http://cxolyris.cxomedia.com/t/2588861/1414060/28439/0/
3. Group to Release New IT Security Metrics. The Center for Information Security is set to release new metrics. Article at: http://cxolyris.cxomedia.com/t/2588861/1414060/28440/0/

Privacy and Security Tip:
Kim Komando suggests the following: External hard drives are a great way to store and transport data. Some of that data could be personal information. You secure important files on your computer so don't forget to do the same for an external hard drive.

An Apple a day…
TidBITS is an Apple oriented e-mail digest worth checking out. Hot Topics in TidBITS Talk/08-Sep-08 by Jeff Carlson has an interesting article link: http://db.tidbits.com/article/9759 titled: "Car Alarm for Stolen Laptops" where Readers suggest a number of laptop-tracking solutions that are available. http://emperor.tidbits.com/TidBITS/Talk/2192

Shocking News...

In light of the active 2008 hurricane season and their havoc on technology requiring electricity, folks are hooking computers to generators. This should be a good solution but generators can produce power surges which if strong enough could maim a system or at least shorten its life expectancy. If the computer gets its power via a battery pack and an AC is run through it before being used, this should smooth the surges out while also recharging the battery. However, if the computer has no battery power source, place a UPS or surge suppressor between the generator and the system to protect it.

Did you hear that the Supreme Court ruled "punishment of criminals violates their civil rights"? ;-)

Upcoming Events

November 17, 2008. Managing and Measuring Operational Risk Course
The Managing and Measuring Operational Risk course in New York City (to be held again in NYC July 7 – 10, 2009) shows how philosophical and operational elements combined with practical tools can ensure effective risk mitigation. This is a participatory and highly interactive course with limited class size. For more information and to register call (212)361-3299 or visit www.euromoneytraining.com/americas**.**

****

January 13 – 16, 2009. Windows Security (Hands On)
Special four day NCAC seminar held at the Arlington Campus of George Mason University. Details will be posted on the ISACA website:
https://isaca-washdc.sharepointsite.com/event_calendar/Lists/Calendar%20of%20Events/DispForm.aspx?ID=245

****

January 27, 2009. Privacy and Security in a Digital World
Covering PCI, Personal Identifying Information, and other related topics, this conference is from 6 to 9PM which includes a Holiday Mixer. Consult the ISACA website for more information: https://isaca-washdc.sharepointsite.com/event_calendar/Lists/Calendar%20of%20Events/All-list.aspx

****

March 11-12, 2009. GovSec Conference
The conference will take place at the Washington DC Convention Center. Its purpose is to provide the highest quality education, training and networking opportunities that establish, enforce and respond to our collective national security interests. Hot topics include:

- Physical security best practices and planning
- Convergence of IT and physical security (focused on real implementations)
- Emerging threats to cyber security
- CBRNE-related topics
- Terrorist thinking and mindset/psychology
- Techniques and tactics for finding and destroying terrorist cells in America
- Infrastructure threat assessment

Information may be found at: http://www.govsecinfo.com/

March 29 – April 1, 2009. Spring World 2009
Disaster Recovery Journal will hold their *Spring World 2009* at Disney's Coronado Springs Resort in Florida. Pre and post courses are also offered. For further information and registration details visit:
https://www.drj.com/index.php?option=com_content&task=view&id=2269&Itemid=735

****

July 7 – 10, 2009. Managing and Measuring Operational Risk Course
This course, to be run in New York City, shows how philosophical and operational elements combined with practical tools can ensure effective risk mitigation. This is a participatory and highly interactive course with limited class size. For more information and to register call (212)361-3299 or visit www.euromoneytraining.com/americas**.**

****

July 10 – 13, 2009. Computing, Communications and Control Technologies: CCCT 2009 Conference
The 7th International Conference on Computing, Communications and Control Technologies: CCCT 2009 (http://www.2009iiisconferences.org/CCCT) will take place in Orlando, Florida. Please refer to the website for further information and registration details.

****

July 10 – 13, 2009. 6th International Symposium on Risk Management and Cyber-Informatics: RMCI 2009
The 6th International Symposium on Risk Management and Cyber-Informatics: RMCI 2009 (http://www.2009iiisconferences.org/RMCI) will take place in Orlando, Florida, USA. Please refer to the website for further information and registration details.

****

Information Resources

FISSEA member, Judith Myerson: available as a subject matter presenter for conferences and meetings on a wide variety of topics. To discuss ideas or opportunities, please contact her at jmyerson@bellatlantic.net

FISSEA member, Toni Taylor: Program Manager for the Defense-Wide voucher management program for Defense Activity for Non-traditional Education Support (DANTES). Defense Information Assurance Program (DIAP) and DANTES have a program and an application (The Personnel Certification Support System (PCSS)) that is being used to manage mandated certifications under directive 8570 and discretionary training and certifications that are offered by the armed services and other agencies. For more information, contact Toni at toni@jasztech.com.

****

Birthday Announcement:

Happy Birthday to the PC Mouse which turned 40 on December 9th! Though the Stanford scientists who named it have often wished it had been a name with less stigmas, Mouse stuck and became the ease of use foundation for what has been the Personal Computer. The next anticipated major cursor mover may be our eyes or brain waves but the beloved Mouse will always have its place in technological history. FISSEA wishes a Happy Birthday to the Mouse.