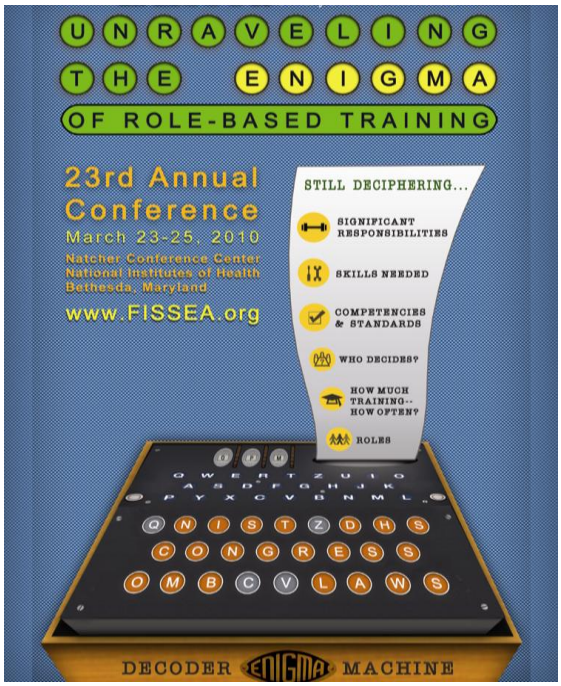
fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

News and Views

Spring Issue March 2010

IN THIS ISSUE



FISSEA 2010 Conference

Unraveling the Enigma of Role-Based Training

FISSEA's 2010 Annual Conference will be held at the National Institute of Health Natcher Conference Center in Bethesda, Maryland on **March 23 – 25, 2010**. The conference will be three days, two tracks with keynotes, panels, presentations, and a vendor exhibition on day two. 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.

Register now at: www.fissea.org!

Congratulations to the 2009 FISSEA Contest Winners!

Gretchen Ann Morris, CISSP
Contest Coordinator, FISSEA

During the 2009 FISSEA conference we announced the winners of our Awareness, Training, and Education contest. We had 23 different entries from 14 different organizations, all of which were of the best quality.

Congratulations again to our winners!

Poster
Jane Moser – Service Canada

Motivational Item
Terri Cinnamon – Department of Veterans Affairs

Web Site
David Kurtz – Bureau of the Public Debt (BPD)

Newsletter
Susan Farrand – Department of Energy

Training Exercise
Christina Painton – DISA, SAIC, and Carney

The winning entries are posted on the FISSEA website and may be found here.

Thanks also to our three judges who worked very hard to ensure that the contest was a success!

FISSEA 12th FREE Workshop

Susan Hansche, CISSP

On December 2nd, we held our 12th Free FISSEA workshop and had over 70 participants (both in person and remotely via webinar) discussing what is currently available and what is needed. The workshop was a precursor to our March 2010 conference where we will have a track dedicated to how agencies can share information and work together to successfully implement information security role-based training.

Here are a few highlights from the FISSEA workshop:

The government has established a central program, Information Systems Security Line of Business (ISS LOB) Tier Two Training (T2T) to encourage agencies to share information assurance, cyber security, and information system security role-based training with each other and to share best practices. The workshop presenters have role-based training programs available (please refer to the FISSEA Web site for contact information).

ISS LOB T2T Thoughts and Discussion Key Points

- There is an interest amongst participants to share training services and products
- More communication about what is available is needed
- Tracking – how, when, what
- FREE – agencies want it for free or little cost – some agencies just do not have training funds
- Identification of who needs role-based training is not consistent
- How can we get an agreement on what are the "top 10" roles across all agencies
- We can get to a solution that offers "baseline" training (75-80% of content that is applicable to all agencies) for some key roles and that would be helpful

Our distance learning expert, Loyce Pailen, recorded the workshop session and has posted the archived sessions on the Web. If you would like to review all or any part of the discussion, please refer to the FISSEA Web site for replay details. If you would like more information on the FISSEA workshops in general, please send an email to Susan Hansche, FISSEA Chair.

PASSING THE CISSP EXAM THE FIRST TIME AND COMPLYING WITH DOD DIRECTIVE 8570

Dr. Victor N. Berlin, President
University of Fairfax

The ***Certified Information Systems Security Professional* (*CISSP*)** certification has become an important credential for managerial information security (infosec) professionals in both the public and private sectors. For instance, in the Department of Defense (DoD) earning the certification helps to ensure compliance with the department's Directive 8570, which requires its information technology employees with elevated network privileges to earn industry certifications, including the CISSP for IT managers.

Many infosec professionals are perplexed by the need to obtain the CISSP certification. Understandably they feel that having multiple years of experience should speak for itself and that obtaining a certification should

not be necessary. However, the growth of continuing-education and professional certification compliance initiatives in public- and private-sector organizations has led many employers to adopt mandatory requirements that their employees earn the CISSP certification.

Of course, the primary obstacle for earning the certification is passing the CISSP exam. One method to help CISSP candidates pass the exam the first time, is to follow a Nine-Step CISSP Exam Preparation Program that incorporates tools offered by a variety of education providers that serve the information security sector.

The first of the nine steps is to complete a self-assessment tool. It is important to note that if a candidate determines that more preparation is warranted before taking the CISSP exam, he or she can enroll in any CISSP preparation program, selecting from among numerous providers that supply each of the tools outlined in the following Nine-Step CISSP Exam Preparation Program.

The Nine-Step CISSP Exam Preparation Program uses widely available tools to help a candidate prepare for the exam:

1. CISSP Self-Assessment Tool to identify his or her strengths and weakness
2. CISSP Exam Prep Clinic for test-taking methods
3. CISSP eLearning for CISSP Common Body of Knowledge (CBK) content review
4. CISSP Text book for in-depth CISSP CBK review of weaker CISSP domains identified by the self-assessment tools
5. CISSP Review Seminar guided by an experienced instructor.

The Nine-Step CISSP Exam Preparation Program provides flexibility for different learning styles and meets the needs of individuals with varying levels of infosec experience. The plan operates as follows:

The Nine-Step CISSP Preparation Program

1. The candidate assesses his or her level of knowledge of the CISSP Domain using a self-assessment tool.
2. The candidate uses a CISSP text book to study CISSP Domains identified as “weak” by the self-assessment.
3. The candidate uses a CISSP eLearning tool to strengthen the “weak” areas.
4. The candidate uses a second CISSP Domain Self-Assessment Tool to assess his or her progress on the weaker CISSP Domains.
5. The candidate uses a CISSP eLearning Tool and the CISSP Text Book to study the “weak” areas in-depth again.
6. The candidate completes a classroom or web-based instructor-led CISSP review seminar of the CISSP Domains.
7. The candidate uses the instructor of the CISSP Review Seminar as a mentor.
8. The candidate uses a third and final CISSP Domain Self-Assessment tool to assess progress and continues studying “weak” CISSP Domains until he or she can pass the entire third CISSP Domain Self-Assessment tool.
9. The candidate completes various online or written “mock” CISSP Exam tests to learn how to analyze CISSP test items in order to improve their test-taking skills.

We have found that if CISSP exam candidates follow this Nine-Step CISSP Exam Preparation Program, they can maximize their chances of passing the CISSP certification exam the first time.

To learn more about the Nine-Step CISSP Exam Preparation Program visit the University of Fairfax CISSP Exam Preparation Web page or contact Juliette Goldman, associate dean of continuing professional education, University of Fairfax, at (703) 962-1622 or at CISSPAdmin@ufairfax.net.

FISSEA Executive Board Members Term 2008-2010	FISSEA Executive Board Members Term 2009-2011
Maria Jones US Department of Labor OSHA jones.maria@dol.gov	**Daniel Benjamin** American Public University dbenjamin@apus.edu
Richard Kurak NASA IT Security Awareness & Training Richard.s.kurak@nasa.gov	**Art Chantker** Potomac Forum, Ltd. art@potomacforum.org
Gretchen Morris DB Consulting Group/NASA ITSATC Gretchen.A.Morris@nasa.gov	**Terri Cinnamon** Department of Veterans Affairs terri.cinnamon@va.gov
Lakshmi Narasimhan East Carolina University narasimhanl@ecu.edu	**Susan Farrand** Department of Energy susan.farrand@hq.doe.gov
Cheryl Seaman National Institutes of Health seamanc@mail.nih.gov	**Susan Hansche** Avaya Govt Solutions/Department of State susan.hansche@avayagov.com
	John Ippolito Allied Technology Group, Inc. ippolitoj@hq.alliedtech.com
Vacancy due to resignation by Emma Hochgesang-Noffsinger	**Mark Wilson** NIST mark.wilson@nist.gov
Other FISSEA Contacts:	
Peggy Himes NIST NIST/FISSEA Co-liaison peggy.himes@nist.gov	**Diane Blocksom** DB Consulting Group/NASA FISSEA Newsletter Editor diane.l.blocksom@nasa.gov

FISSEA List Serve:

The NIST Computer Security Division 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.Blocksom@nasa.gov with the 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 Diane Blocksom Diane.L.Blocksom@nasa.gov . Please place "FISSEA Trainia Submission" in the Subject line.

~~~~~~

FISSEA's 23rd Annual Conference – Register Today!

FISSEA's 2010 Annual Conference will be held at the National Institute of Health Natcher Conference Center on **March 23 – 25, 2010**. The conference will be three days, two tracks with keynotes, panels, presentations, and a vendor exhibition on day two. 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.

Visit the FISSEA website for agenda and registration information. If you have any questions relating to our 2010 Conference, please address them to Captain Cheryl Seaman, seamanc@mail.nih.gov, Conference Director.

~~~~~~

Security Awareness Collaboration on LinkedIn

Melissa Guenther (mguenther@cox.net) is using LinkedIn to start a collaborative platform for a Security Awareness Change Management Plan. The Group in LinkedIn is called Security Awareness Protect-Detect-React. If you would like to sign up as a part of this group please email Melissa at mguenther@cox.net. For more information, visit The Information Warfare Site.

~~~~~~

NIST Update

The NIST Computer Security Division, FISMA Implementation web site provides details of its objectives, services, and projects. The most recent announcements are below:

January 2010

Special Publication 800-38E: *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices* has been released. This publication approves the XTS-AES mode of the AES algorithm by reference to its specification in IEEE Std 1619-2007, as an option for protecting the confidentiality of data on storage devices.

New Milestone Schedule

The NIST FISMA Implementation Project has announced a new milestone schedule for its key publications in development or undergoing modification. The revised milestone schedule for Phase I reflects the ongoing work with the Joint Task Force Transformation Initiative and the priorities established by the participating partners representing
~~~~~~

the Department of Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and NIST. These publications include:

- **SP 800-30, Revision 1**: *Guide for Conducting Risk Assessments* (Formerly *Risk Management Guide for Information Technology Systems*), (Projected Final: August 2010)
- **SP 800-37, Revision 1:** *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Formerly *Guide for the Security Certification and Accreditation of Federal Information Systems*), (Final: February 2010)
- **SP 800-39:** *Integrated Enterprise-wide Risk Management: Organization, Mission, and Information Systems View* (Formerly *Managing Risk from Information Systems: An Organizational Perspective)*, (Projected Final: August 2010)
- **SP 800-53A, Revision 1:** *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, (Projected Draft: April 2010)

In addition the Phase II schedule was updated on November 5, 2009, including:

- **RMF Training:** *Initial Risk Management Framework (RMF) Training Module* (Projected Final: April 2010)
- **RMF Web-based Training:** *Initial Web-based Risk Management Framework (RMF) Training Module* (Projected Draft: May 2010)
- **RMF FAQs & QSGs:** *Frequently Asked Questions (FAQs) and Quick Start Guides (QSGs) for the Select, Implement, Assess and Authorize Steps of the Risk Management Framework* (Projected Draft: by April 2010)

NIST Releases Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
February 22, 2010

NIST announces the final publication of **Special Publication 800-37, Revision 1**, *Guide for* Applying *the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. This publication represents the second in a series of publications being developed under the auspices of the Joint Task Force Transformation Initiative. For the past three years, NIST has been working in partnership with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to develop a common information security framework for the federal government and its contractors. The initial publication produced by the task force, NIST Special Publication 800-53, Revision 3, created a common security control catalog reflecting the information security requirements of the national security community and the non-national security community. NIST Special Publication 800-37, Revision 1, continues the transformation by changing the traditional process employed by the federal government to certify and accredit federal information systems. The revised process provides greater emphasis on: (i) building information security capabilities into information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) understanding and accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of information systems.

NIST Special Publication 800-37, Revision 1, is the full transformation of the Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF). The RMF-based process has the following characteristics:

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation and automated support tools to provide senior leaders the necessary information to take credible, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security more closely into the enterprise architecture and system development life cycle;
- Provides equal emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;

- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls); and
- Links risk management processes at the information system level to risk management processes at the organization-level through a risk executive (function);

The risk management process described in this publication changes the focus from the traditional stove piped, static approaches to C&A and provides the capability to more effectively manage information system-related security risks in highly dynamic environments of complex and sophisticated cyber threats, ever increasing system vulnerabilities, and rapidly changing missions. In addition to the above changes, NIST Special Publication 800-37 revises information system authorization guidance for federal agencies and extends the current approach to include joint and leveraged authorizations.

Database Application for NIST SP 800-53 Security Controls Available
The NIST Special Publication 800-53 Revision 3 Reference Database Application can be downloaded and contains the catalog of security controls from Appendix F and G of the SP 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009). The database application has been posted to two locations http://csrc.nist.gov/publications/PubsSPs.html {entry following "SP 800-53 Rev 3 Aug 2009 Recommended Security Controls for Federal Information Systems and Organizations (*Errata as of 09-14-2009*) sp800-53-rev3-final-errata.pdf "}; and http://csrc.nist.gov/groups/SMA/fisma/support_tools.html The Support Tools section under Resources from the FISMA Implementation Project homepage.

The database application has been developed primarily to help customers quickly and efficiently:

- **Browse** the security controls, control enhancements, and supplemental guidance, including summarizing by control class, control family and control impact baseline;
- **Search** the security control catalog using user-specified keywords; and
- **Export** the security control-related information in the database application to other popular data formats (e.g., .dbf, .xls, .htm, .xml, .csv) that can be used in various tools and applications.

The information in the database is ***read only*** and can be viewed or extracted, but cannot be updated or modified using this application.

PLEASE NOTE: To install, extract the zip archive in a directory where the user has read, write, and execute permissions; open the SP_800-53_Rev-3_DB-R1.4.0-BETA directory; and double-click the SP_800-53_Rev-3_DB-R1.4.0-BETA.exe file to run the application. To simplify use, the application has been updated removing the request for a user name and password when the application is executed. The zip file may be found under the FISMA home page; Resources; Support Tools; <http://csrc.nist.gov/checklists/SP_800-53-Rev3_DB-R1.4.0-BETA.zip>

NIST LINKS
The NIST CSRC Special Publications website is http://csrc.nist.gov/publications/PubsSPs.html.
The NIST FISMA Implementation Project website is located at: http://csrc.nist.gov/groups/SMA/fisma/.

~~~~~~

Free CISSP Assessment Tool

Dr. Victor N. Berlin, President of the University of Fairfax, is offering a CISSP self-assessment tool – for free!

The University of Fairfax's free online CISSP Self-Assessment Tool will help you to decide if you are ready to take the exam. If you are not ready, it will identify which of the 10 CISSP domains that you need to study more before sitting for the exam.

Other features of this helpful self-assessment tool are:

- An online sample of University-developed practice exams,
- Sample exam questions covering all 10 CISSP domains,
- Multiple retakes spanning a three-week period, and
- 24/7 access.
~~~~~~

This CISSP Self-Assessment Tool is the first step along the path to passing the CISSP exam. Click here to try this free tool online today. For more information contact Juliette Goldman, associate dean of continuing professional education, University of Fairfax, at (703) 962-1622 or at CISSPAdmin@ufairfax.net.

~~~~~~

Tidbits

Looking for a way to enhance your security awareness program?

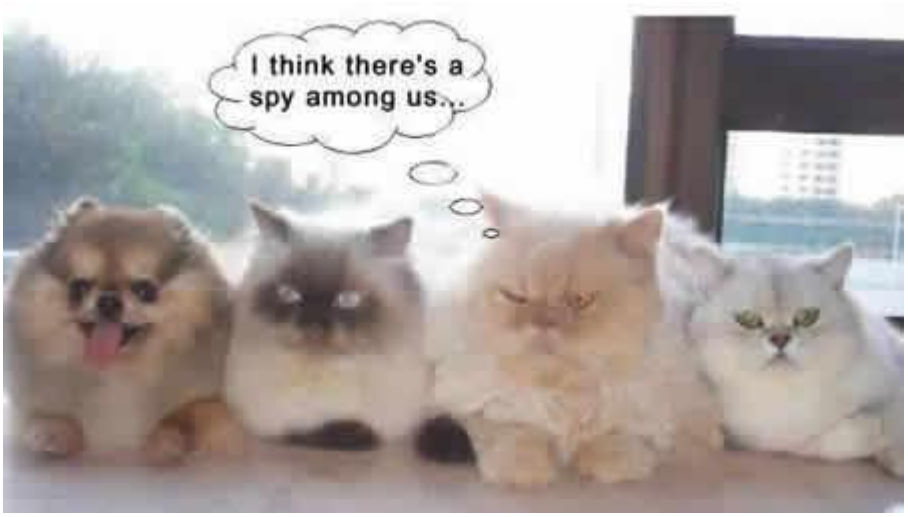
- OnGuardOnline.gov provides practical tips from the federal government and the technology industry. Security-related topics are explained not only by content, but also by games and videos to enhance the experience. Some of the games and videos are free to use on your own website.
- GetNetWise is a project of the Internet Education Foundation and delivers resources people need to make informed decisions about their family's use of the Internet.
- StaySafeOnline.org by the National Cyber Security Alliance breaks down security-related topics by academia, home, and small business offering tools and resources to help use the Internet securely and safely.
- iKeepSafe.org presented by the Internet Keep Safe Coalition comprised of a broad partnership of government and industry leaders working together for the health and safety of youth online.

~~~~~~

Extras

September 30, 2009 – Hillsboro police told the Associated Press that a bank robbery attempt failed after a teller told the woman who handed her a threatening note that she couldn't read the handwriting.
October 12, 2009 – A man caught with more than 1,700 pounds of pot on his person tried to hide the scent with limes according to the Asheville Citizen Times.
November 6, 2009 – A drive-by shooting failed in Appleton, Wisconsin, because the driver forgot to roll down his window!

~~~~~~


~~~~~~

Upcoming Events

Here are just a few of the upcoming events happening this year. Click on the host name to get more information about the event.

DATE		HOST	EVENT	LOCATION
March	**1 – 5**	RSA	RSA Conference 2010	San Francisco, CA
March	**6 – 15**	SANS	SANS 2010	Orlando, FL
March	**15 – 16**	ASIS	2010 Spring Conference	Washington, DC
March	**23 – 24**	FISSEA	FISSEA's 23rd Annual Conference "Unraveling the Enigma of Role-Based Training"	Bethesda, MD
March	**23 – 24**	GovSec	U.S. Law Conference & Expo	Washington, DC
April	**12 – 14**	ASIS	Managing Your Physical Security Program	New Orleans, LA
April	**13 – 15**	NIST	9th Symposium on Identity and Trust on the Internet (IDTrust 2010)	Gaithersburg, MD
April	**17 – 23**	MIS	Infosec World 2010	Orlando, FL
April	**18 – 22**	ISACA	Computer Audit, Control and Security (CACS) Conference	Chicago, IL
April	**26 – 28**	NSI	Impact 2010	Chantilly, VA
May	**26 – 27**	CSI	Security for Business Agility	San Francisco, CA
June	**6 – 9**	ISACA	International Conference	Cancun, MX
June	**6 – 14**	SANS	SANSFIRE 2010	Baltimore, MD
September	**13 – 15**	ISACA	Information Security and Risk Management Conference	Las Vegas, Nevada
September	**15 – 17**	ISSA	ISSA International Conference Connect & Collaborate	Atlanta, Georgia
September	**20 – 22**	HTCIA	HTCIA International Training Conference & Expo	Atlanta, Georgia
October	**6 – 8**	ISACA	IT Governance, Risk and Compliance Conference	Boston, Massachusetts

~~~~~~

The man who smiles when things go wrong has thought of someone to blame it on.
Robert Bloch
~~~~~~