How You Will Benefit

Comply with the Federal Information Security Management Act and Associated Audits

Explore a step-by-step walkthrough of the FISMA process and prepare for IT system audits

Conduct a Comprehensive Risk Assessment

Identify and mitigate security risks and vulnerabilities in complex information systems

Develop an IT System Security Plan

Utilize NIST guidance to maximize the integrity of your agency's information

Create a Streamlined and Cost-Efficient FISMA Process

Establish a cost-efficient, streamlined and verifiable process for FISMA reports

Plus!
Wireless Security Symposium
September 14, 2005

Acquire the Latest Solutions and Best Practices in Wireless Security!

- ✔ Manage and Mitigate New Wireless Threats
- ✔ Prepare for Wireless Security Audits
- ✔ Develop a Business Case for Wireless Security
- ✔ Establish Effective Policies and Training Procedures

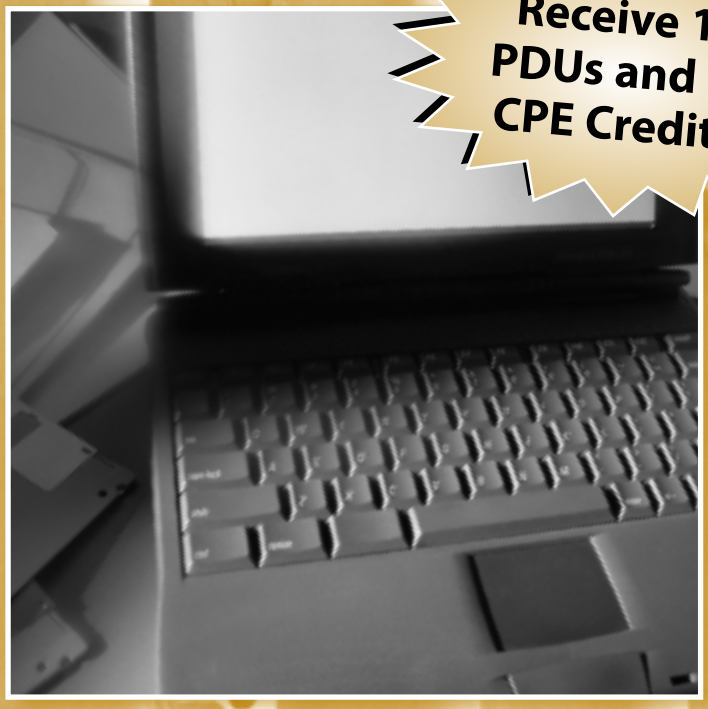
Resolve Key Privacy and Identity Theft Concerns!

Information Security Management

FISMA GUIDANCE SIMULATION 2005

September 14-16, 2005
The Performance Institute • Arlington, VA

Receive 13 PDUs and 13 CPE Credits!



Presented by:

The Performance Institute

Prepare for and Achieve Compliance for New Security Audits

www.PerformanceWeb.org

Information Security Management in Government

September 14-16, 2005 • The Performance Institute • Arlington, VA

PRE-EVENT WIRELESS SECURITY SYMPOSIUM

September 14, 2005

Vulnerabilities Plague Wireless Networks

"The most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot." -NIST Special Publication 800-48

Government agencies still face many challenges in securing conventional wired networks, leaving few remaining resources to tackle the many critical threats unique to wireless networks. While the Federal Information Security Management Act (FISMA) requires that all agencies report to OMB annually, GAO has recently released a daunting report showing little progress on securing WIFI and Bluetooth Technologies. This interactive, hands-on, and methodology-based symposium promises to deliver the latest best-practices and cutting edge solutions in:

- ✔ FISMA Reporting and Generation Requirements
- ✔ Wireless Security Threats and Controls
- ✔ LAN Security Checklist
- ✔ Business Case Development
- ✔ Model Network Configuration Requirements
- ✔ Verifiable Security Documentation for WLAN Audits
- ✔ GAO Standards for Wireless Security
- ✔ Immediate Threat Mitigation Techniques

PRE-EVENT AGENDA

9:00 Updates on the Latest NIST Standards, FISMA Requirements and GAO Guidelines for Wireless Security
- Explore how the new FISMA guidance addresses wireless network security
- Learn new GAO standards for improving wireless security
- Understand NIST SP 800-58

10:00 Trends Dialogue: Pay Now or Pay Later: Resolving Critical Gaps in Wireless Security
- Hear from agency executives on practical steps needed in tackling pressing challenges
- Understand the true scope of wireless security weaknesses in government

11:30 The Next Generation of Wireless Threats: Security for Mobile and Handheld Technologies
- Examine new technologies that bring increased threats and new vulnerabilities
- Keep pace with the emerging threats by analyzing the future of cybercrime

12:15 Networking Luncheon and Peer Solutions Exchange

1:00 Privacy Concerns and Identity Theft: Developing Effective Agency Procedures and Training Standards
- Acquire the latest agency best practices for developing standards and procedures in addressing privacy concerns
- Learn valuable techniques for establishing a training and awareness program in your agency

2:00 Understanding the Wireless Security Audit Process: Delivering Increased Transparency and Accountability to Auditors
- Work with your inspector general to implement verifiable security controls aligned with common auditing standards
- Discover key successes and pitfalls of automating the FIMSA process in a wireless environment

2:45 Securing Budget Funds: Building a Comprehensive Business Case for Wireless Security
- Utilize the latest business case tools and strategies to achieve full executive "buy in" for your wireless security initiatives
- Strengthen business cases with effective solutions, proven project management skills, and verifiable security controls

3:30 Application Workshop: Step-by-step walkthrough of NIST SP 800-48 Standards
- Implement key security controls using a step-by-step approach for aligning with NIST standards
- Develop a wireless LAN and handheld device security checklist
- Explore key risk mitigation techniques described in NIST SP 800-48

5:00 Adjourn

** Certain topics follow guidance from the National Institute for Standards and Technology*

PROGRAM AGENDA

Day One: September 15, 2005

9:00 Overview of Current Information Security Guidelines and Requirements
- Federal Information Security Management Act (FISMA)
- Emerging Guidance from Office of Management and Budget and the National Institute for Standards and Technology (NIST)

10:00 Understand Security Terminology and Identify Employee Roles
- Examine the use of key security controls including cryptography, authentication, firewalls, enterprise system monitoring and IT systems security posturing
- Identify key security safeguards and their relationship with various business processes
- Assign security responsibilities for staff at the management and operational level

1:00 Information Security within a Performance Framework
- Use the Government Performance Logic Model to determine outcome-oriented performance measures for security controls
- Implement the Logic Model to align your budget with results and integrate a strategic plan

Information Security Management in Government

September 14-16, 2005 • The Performance Institute • Arlington, VA

Step-By-Step Walk through of FISMA Requirements and Supporting Guidance

2:15 Step 1: Categorization Standards
- Develop standards to categorize information and information systems based on risk level and information sensitivity
- Use categories to determine appropriate information security controls

3:00 Step 2: Mapping Guidelines
- Identify information and information systems to be included in each category
- Plan for specific security controls necessary for each category

3:30 Step 3: Minimum Security Requirements
- Determine and implement minimum security requirements that align with each part of the business process
- Utilize established requirements to select, implement and manage various IT services

Day Two: September 16, 2005

9:00 Step 4: Applying a Risk Management Framework
- Utilize NIST guidelines and publications to apply an integrated risk assessment
- Implement eight steps to manage, track and minimize risk in IT projects

10:30 Step 5: Implement a System Security Plan
- Benchmark current security controls against mandatory requirements
- Develop a plan for implementing controls necessary to close remaining security gaps

1:00 Step Six: Certification and Accreditation
- Conduct a thorough assessment of management, operational and technical aspect of information systems
- Discover lessons learned from existing evaluation and validations programs

2:30 APPLICATION WORKSHOP: Develop a Security Assessment Report
- Implement the six-step process to develop a complete security assessment report in compliance with FISMA requirements
- Understand the key elements of a high scoring report

4:30 Adjourn

KEY METHODOLOGIES COVERED

Attend this training to implement a seven-step management process necessary to comply with key FISMA requirements. Utilizing NIST guidance and mandates as a framework for implementing comprehensive security controls, apply key countermeasures necessary to ensure the integrity of your agency's information systems. Next, implement the Government Performance Logic Model to measure the performance of applied safeguards.

6 Steps to Implementing Effective Security Standards

Step 1:	Categorization Standards	Step 4:	Risk Management Framework
Step 2:	Mapping Guidelines	Step 5:	System Security Plan
Step 3:	Minimum Security Requirements	Step 6:	Certification and Accreditation

RECEIVE CERTIFICATION & IN-HOUSE TRAINING

This event is part of the Government Performance Management Certification Program. In addition, the Performance Institute offers customized education programs to federal and state agencies that wish to train staff members in their own facility on diversity recruitment. For more information about the certification and in-house training options available to you, please contact Blake Zach at 703-894-0481 or Zach@performanceweb.org.



Venue and Hotel:

Information Security Management in Government will be hosted at the Performance Institute in Arlington, Virginia, just one block east of the Courthouse stop on the orange line of the D.C. Metro. A public parking garage is located inside of the building. Continental breakfast and a catered lunch will be provided for delegates on each day.

The Performance Institute
1515 N. Courthouse Rd., Suite 600, Arlington, VA 22201
703-894-0481

A limited number of rooms have been reserved at a discounted rate of $153 at the Holiday Inn Rosslyn at the Key Bridge. Please contact the hotel directly and use the code ILCORPER when making reservations at the hotel.

Holiday Inn Rosslyn at the Key Bridge
1900 North Fort Myer Drive
Arlington, VA 22209
1-800-368-3408
www.holiday-inn.com/rosslynkbridge

Tuition and Group Discounts:

Information Security Management: FISMA Simulation 2005 (T199):	$895
Wireless Security Symposium (T204):	$295

Reduced tuition rates for delegates who attend in groups of three or more are also available by calling Melvin Hall at 703-894-0481 or email him at Hall@PerformanceWeb.org.

Cancellations and Quality Assurance:

The Performance Institute strives to provide you with the most productive and effective educational experience possible. If after completing the course you feel there is some way we can improve, please write your comments on the evaluation form provided upon your arrival. Should you feel dissatisfied with your learning experience and wish to request a credit or refund, please submit it in writing no later than 10 business days after the end of the training to: Chris DeMaio, Chief Operating Officer, The Performance Institute, 1515 N. Courthouse Road, Suite 600, Arlington, VA 22201 (phone: 703-894-0481). We will evaluate individual complaints in a context of collective comments from the event. **Note:** A $150 service fee will be charged on cancellations received less than three weeks from the date of the event. A credit memo will also be sent reflective of that amount, which can be used for a future Performance Institute conference.

Information Security Management in Government

September 14–16 • The Performance Institute • Arlington, VA

REGISTRATION FORM

To Register:

PRIORITY CODE: T199-WEB

1. Call Melvin Hall at 703-894-0481
2. visit www.performanceweb.org
3. or fax this form to 703-894-0482

☐ **Yes! Please register me for the Information Security Management in Government Summit AND the Wireless Security Symposium (T199 & T204)**

☐ **Yes! Please register me for the Information Security Management in Government Summit (T199)**

☐ **Yes! Please register me for the pre-event Wireless Security Symposium (T204)**

DELEGATE INFORMATION

NAME

TITLE

ORGANIZATION

ADDRESS

CITY STATE ZIP

PHONE

FAX

E-MAIL

METHOD OF PAYMENT

☐ Check ☐ Purchase Order/Training Form ☐ Credit Card

NAME ON CARD

CARD NUMBER EXPIRATION

CPE Credit:
Delivery Method: Group-live
Program Level: Intermediate
Prerequisites: None
Advanced Preparation: None

National Registry of CPE Sponsors
CPE Credits: 13

The Performance Institute is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Avenue North, Nashville, TN 37219-2417. Website: www.nasba.org

PMI Registered Education Provider
PDUs: 13

The Performance Institute has been reviewed and approved as a provider of project management training by the Project Management Institute. As a PMI Registered Education Provider (R.E.P), The Performance Institute has agreed to abide by PMI established quality assurance criteria. "PMI" and the PMI logo are service and trademarks registered in the United States and other nations; "PMP" is a certification mark registered in the United States and other nations; "PMBOK" and "CAPM" are trademarks registered in the United States and other nations by the Project Management Institute, Inc., which is not affiliated with The Performance Institute.