



## **GTRA SecureGOV Council Meeting**

December 4 - 6, 2011  
Bedford Springs Resort; Bedford, PA  
[www.SecureGOV.info](http://www.SecureGOV.info)

*This PDF Includes Featured Sessions, Curriculum, Schedule of Events, and Registration Form*

### **Featured Sessions**

#### **Update from Office of Cybersecurity and Communication**

**Roberta Stempfley**, Director, National Cyber Security Division, **DHS**

#### **The Future Directions of Cyber Security and Risk Management**

**Honorable Theresa Grafenstine**, Inspector General, **United States House of Representatives**  
**Dr. Ronald Ross**, Senior Fellow, **NIST**

#### **Reducing Spend while Enhancing Information Protection**

**Dr. Paul A. Tibbits**, Deputy Chief Information Officer, Office of Architecture, Strategy and Design, **VA**

#### **Taking your ICAM investments to the next level**

**Deborah Gallagher**, Acting Director, Identity Management Division, Office of Government Policy, **GSA**  
**Chase Garwood**, Chief Technology Officer, **US-VISIT**

#### **Using Innovation to Establish Enterprise-wide Security**

**Benjamin Bergersen**, Chief Information Officer, Office of the Inspector General, **Commerce**  
**Mary Davie**, Assistant Commissioner, Federal Acquisition Service, Integrated Technology Services, **GSA**  
**Vaughn Noga**, Chief Technology Officer and Director, Office Technology Operations and Planning, **EPA**  
**Philip Wenger**, Deputy Policy Lead, Budget Line of Business, **OMB**

#### **The NIST Cloud Reference Architecture and Security Considerations**

**Peter Mell**, Senior Computer Scientist, Computer Security Division, **NIST**

#### **Top Security Reports and Resources from GAO**

**Gregory Wilshusen**, Director IT Security Issues, **GAO**

#### **Consolidate without Compromising Security**

**Joe Albaugh**, Chief Information Security Officer, **FAA**  
**Carmen Iannacone**, Chief Technology Officer, **Smithsonian Institution**  
**Richard Boe**, Manager, Infrastructure Services Delivery Group, Air Traffic Organization, **FAA**

#### **Fostering true CIO/CISO Collaboration to become a Center for Excellence**

**Philip Ferraro**, Chief Information Security Officer, **FCC**  
**Robert Naylor**, Chief Information Officer, **FCC**

#### **How to Operationalize NIST Recommendations**

**Marian Cody**, Chief Information Security Officer, **HUD**



### **Securely Deploying iPad, iPhones and other Mobile Devices on your Network**

**Reggie Brown**, Deputy Associate Director, Emerging Solutions/HR Innovations, **OPM**

**Noah Nason III**, Chief Technology Officer, **ATF**

**Jerry Horton**, CIO, **USAID**

**Matt Wilkinson**, PM, iPad Pilot, **NIST**

### **System Consolidation at NRC: A Case Study**

**Pat Howard**, Chief Information Security Officer, **NRC**

### **Using Shared Services to Improve and Secure Government**

**Andrew Schoenbach**, Chief, MAX Budget Systems, Budget Line of Business Policy Lead, **OMB**

### **800-53 Privacy Appendix: What it Means and how it Affects You**

**Jonathan Cantor**, Chief Privacy Officer & Director of Open Government, **Commerce**

**Thomas Boyce**, Deputy Chief Information Officer and Chief Privacy Officer, **NRC**

### **Secure Information Sharing in a Growing Hostile Environment**

**Richard Russell**, Deputy G-2, Senior National Intelligence Service, **Army Materials Command**

### **Changing Culture to support Security**

**Jirka Danek**, Chief Technology Officer and Chief Information Security Officer, **Shared Services Canada**

**Con Kenney**, Senior Research Fellow, Information Resource Management College, **NDU**

**Lori Herrington**, Chief, Field Detachment Security Directorate, **Defense Contract Audit Agency**

**Dan Gragg**, Director of Security, Navy Special Access Program Central Office, **Navy**

### **Best Practices for Responsible, Mission-Focused Social Media Programs**

**Kathy Harman-Stokes**, Chief Privacy Officer, **CFTC**

### **IT Security Dashboards**

**Janet Haase**, Chief Information Officer, Defense Commissary Agency, **Defense**

### **Security Beyond the Device**

**Henry "Bud" Horton**, Security Executive, **ExteNet Systems Inc**

### **Leveraging Industry/Government Partnerships to Reduce Costs while Improving your Security Posture**

**Rob Roy**, CTO, Federal Division, **HP Enterprise Security Products**

**Andy Thurai**, Chief Architect, Intel Application Security and Identity Products, **Intel**

**David Lingenfelter**, Security Officer, **MaaS360 by Fiberlink**

**Centrify**

**Q1 Labs**

### **Other Confirmed Speakers Include:**

**Wolf Tombe**, Chief Technology Officer, **Customs and Border Protection**



## **Boardroom Meetings**

*Boardroom Meetings are unique opportunities that facilitate Government-to-Industry Collaboration a non-sales, non-hostile environment. Throughout the GTRA Council Meeting, groups of government and industry executives participate in 35-minute boardroom meetings designed to foster productive, strategic discussions on various issues facing the government IT community.*

### **Next-Generation Spam Blockers**

**Abaca Technology Corporation**

### **Securing Cross-platform Systems and Applications Leveraging Active Directory** **Centrify**

### **Securing Your Mobile Network**

**ExteNet Systems, Inc.**

### **Continuous Monitoring of Laptops and Smart Devices**

**MaaS360 by Fiberlink**

### **Intelligent Risk Management – Protecting your Enterprise, Cloud and Mobile Capabilities**

**HP Enterprise Security**

### **Federal Cloud Security Initiatives - Choosing the Right Standards and Technologies**

**Intel**

### **Strategies to Stop Zero-Day Attacks**

**Invincea**

### **Live Demonstration - Continuous Monitoring**

**Lumension Security**

### **Know Everything, Answer Anything: A Revolutionary Approach to Network Monitoring**

**RSA NetWitness**

### **Security Intelligence for Government Agencies**

**Q1Labs**



## **Curriculum**

### **Cloud Security**

- Interactive sessions on the most important Cloud security such as: Private/Public/Hybrid Clouds, Acquisition & Outsourcing, Cloud Technologies and the integrity of your agency/department's security when moving to the Cloud.
- Focus on government Cloud programs/initiatives including Cloud First, FedRAMP, Cloud Security Assessment Methodologies and other guidance documents from NIST
- Situational examples and case studies will share best practices and lessons learned from agencies who have deployed secure Cloud solutions

### **Risk & Incident Management: Prevention, Detection, Response**

- Interactive discussions on how to prevent the compromise of your networks/applications/data, and what to do before/during/after an attack
- Review of civilian/intelligence/defense collaborative efforts to create government-wide standards to combat cyber security and Defend Cyber Space during a time where cyber attacks are increasing sophistication and frequency
- Case studies and programs on issues including vulnerability assessments, data breaches, insider threats and malware

### **Identity, Credential, and Access Management**

- Case studies on how PIV systems can be integrated to provide physical and logical access to building/networks within and across government agencies
- Discussion of how cloud computing and shared service initiatives are changing the way agencies must manage access to data and the identities of users
- Overview of new identity management initiatives including the Identity Ecosystem and National Strategy for Trusted Identities in Cyber Space (NSTICS)

### **Mobile Network & Device Security**

- Case Studies, lessons learned and new technologies for securing mobile networks and devices including laptops, flash drives, PDAs, and tablets with special discussions on iPhones, iPads and Android device security
- Interactive discussions on programs, policies and best practices to balance mobile workforce demands for access to mission critical data with security concerns.
- Learn how agencies are using mobile apps and systems to securely deliver better services to citizens, business owners, and employees, including the DoT "WIN" initiative

### **CIO, CTO and Enterprise Architecture's Role in Security**

- CXONON-SECURITY EXECUTIVE EDUCATION on critical security topics
- Discuss best practices to increasing collaboration between CIO, CTO, EAs and CISO departments.
- Case studies of how EA's and CISOs work together to ensure security of all investments, networks and IT projects
- Learn how to effectively communicate the importance of security to non-security focused IT professionals

### **Continuous Monitoring**

- Learn how agencies are using new technologies and policies to improve security through continuous monitoring of networks and vulnerabilities
- Hear updates from NIST on new continuous monitoring guidance and programs including FedRAMP,

### **Innovation in Cybersecurity**

- Discussions on the latest technologies, programs, and processes aimed at improving the government's ability to protect its digital assets
- Particular focus on moving from Reactive to Proactive Security, Security Supply Chain Management, Security Implementation Plans and new C&A processes



## **Office of Cybersecurity and Communication (DHS) and NIST Updates**

- CS&C supports the Office of the Assistant Secretary for Cybersecurity and Communications (DHS) through its divisions which include the National Cyber Security Division and the U.S. Computer Emergency Readiness Team (US-CERT)
- Hear updates from senior leadership on various programs, mandates, regulations, and laws which will affect all public and private sector security professionals
- Learn about NIST security programs including the updates on Risk Management Frameworks, the National Strategy for Trusted Identities in Cyber Space (NSTICS), and National Initiative for Cybersecurity Education (NICE)

## **Secure Information Sharing**

- Discussion of how security technologies and policies can help ensure acceptable levels of risk for your information sharing initiatives, including identity/access management, biometrics, secure shared services, and continuous monitoring
- Discussions and case studies on secure information sharing initiatives and programs throughout the defense/intelligence/civilian communities
- Hear from established information sharing programs such as NIEM and PM-ISE on best practices and lessons learned regarding technology and policy implementation aimed at secure information sharing

## **Technical Briefs on:**

- Advanced Persistent Threats
- Malware
- Data Breaches
- Vulnerability Assessments
- Security Lifecycle Management
- Forensics
- Virtualization of Security Platforms
- Insider Threats
- FISMA
- Controlled Unclassified Information
- Data at Rest
- Data Center Consolidation & Security

## **Secure Social Media**

- A look at security concerns with the use of Social Media and other Web 2.0 technologies and what can be done to minimize risk and exposure
- Discussion and case studies from senior agency and department leaders on how to ensure security is taken into consideration from the onset of all IT infrastructure & architecture investments
- Learn how shares data centers can be created and used while maintaining appropriate levels of risk

## **Collaboration Initiatives for Cyber Security**

- Detailed case studies sharing best practices on how Defense, Intelligence and Civilian agencies are successfully collaborating on various security challenges
- Discuss strategies for Government and Industry to collaborate on common goals and objectives related to security

## **Supply Chain Management**

- Learn from Industry and Government Experts as they discuss the relatively new issue of security supply chain management
- Hear how proper management of contractors and outsourced applications is critical in ensuring security in your agency supply chain

## **Privacy**

- Hear case studies and lessons learned from Chief Privacy Officers on their collaboration with the Security, EA and CIOs office and learn best practices to ensure Privacy standards are maintained in all technology initiatives
- Update on the FEA-Security and Privacy Profile and the critical role EA and Security Architectures play in Privacy
- Hear updates on E-Discovery requirements facing agencies and learn about new technologies and solutions to meet these needs
- Discuss Privacy concerns as it relates to Social Networking, Open Government, Transparency and Web 2.0

## **Cyber Security Professional Recruiting**

- Learn best practices on how to attract and retain top talent for your cyber security program
- Discuss strategies, challenges and success stories with other executives facing similar cyber security recruiting challenges



## **Schedule of Events**

### **Sunday December 4, 2011**

11:00 am - 1:00 pm: Registration & Arrival Luncheon  
1:00 pm - 2:00 pm: Strategic Knowledge Exchange  
2:25 pm - 4:30 pm: Executive Sessions  
4:30 pm - 6:00 pm: Free Time  
6:00 pm - 7:00 pm: Networking Cocktail Reception  
7:00 pm - 8:30 pm: Dinner & Opening Keynote Address

### **Monday December 5, 2011**

6:30 am - 7:30 am: Breakfast  
7:30 am - 8:30 am: Opening Keynote Address  
8:45 am - 10:40 am: Roundtable Collaboration Meetings  
11:00 am - 11:50 am: Executive Meetings  
12:00 pm - 1:00 pm: Luncheon Keynote Address  
1:15 pm - 2:05 pm: Executive Meetings  
2:20 pm - 4:15 pm: Roundtable Collaboration Meetings  
4:35 pm - 5:35 pm: Keynote Presentation  
5:35 pm - 7:30 pm: Free Time  
7:30 pm - 11:00 pm: "Pirates of GTRA" Casino Night Dinner & Entertainment

### **Tuesday December 6, 2011**

7:00 am - 8:00 am: Breakfast  
8:00 am - 9:00 am: Opening Keynote Address  
9:10 am - 10:45 am: Roundtable Collaboration Meetings  
11:00 am - 12:00 pm: Executive Meetings  
12:10 pm - 1:10 pm: Luncheon Keynote Address  
1:30 pm - 4:30 pm: Afternoon Workshop

