

**2008 GFIRST NATIONAL CONFERENCE**  
**ORLANDO, FLORIDA | JUNE 1–6, 2008**

**Uniting the Cyber Response Community**

**AGENDA**

<b>Sunday, June 1 (Pre-Registration)*</b>	
12:00 p.m. - 4:00 p.m.	Registration Open
<b>Monday, June 2 (Pre-Conference Training)*</b>	
7:00 a.m. - 5:00 p.m.	Registration Open
8:00 a.m. - 12:00 p.m.	Pre-Conference Training Sessions Part I
Training Session 1:	<i>Introduction to Control Systems for IT Security Professionals</i>  (8 hour class with lunch break)
Training Session 2:	<i>Intermediate Control Systems Security**</i>  <i>Hands-on format - Intermediate Technical Level</i>  James Lee, Cyber Security Researcher, Idaho National Laboratory  Kenneth Rohde, Cyber Security Researcher, Idaho National Laboratory  (Limited to 35 people) (8 hour class with lunch break)
Training Session 3:	<i>InfraGard Congress</i>  (InfraGard Chapter Members Only)
Training Session 4:	<i>Internet Health Service (IHS) Training</i>  (Closed Session: Only Federal Employees and/ or Contractors)
12:00 p.m. - 1:00 p.m.	Lunch Break
1:00 p.m. - 5:00 p.m.	Pre-Conference Training Sessions Part II
Training Session 1:	<i>Introduction to Control Systems for IT Security Professionals</i>

<p><b>Training Session 2:</b></p>	<p><b><i>Intermediate Control Systems Security**</i></b></p> <p><b><i>Hands-on format - Intermediate Technical Level</i></b></p> <p><b>James Lee</b>, Cyber Security Researcher, Idaho National Laboratory</p> <p><b>Kenneth Rohde</b>, Cyber Security Researcher, Idaho National Laboratory</p> <p><b>(Limited to 35 people)</b></p>
<p><b>Training Session 3:</b></p>	<p><b><i>InfraGard Congress</i></b></p> <p><b>(InfraGard Chapter Members Only)</b></p>
<p><b>Training Session 4:</b></p>	<p><b><i>Analysts Jam</i></b></p> <p><b>(Closed Session: Only Federal Employees and/ or Contractors)</b></p>
<p><b>Pre-Conference Training Sessions CHIPS</b></p>	
<p><b>1:00 p.m. - 1:30 p.m.</b></p>	<p><b><i>New CHIP Welcome and Orientation</i></b></p> <p><b>Michael M. Dubose</b>, Chief, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>Robert M. Moore</b>, Assistant Director, Office of Legal Education, Executive Office for United States Attorneys, U.S. Department of Justice, Columbia, South Carolina</p> <p><b>Mark L. Krotoski</b>, National Computer Hacking and Intellectual Property (CHIP) Program Coordinator, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>(CHIPS ONLY)</b></p>
<p><b>1:30 p.m. - 2:45 p.m.</b></p>	<p><b><i>How the Internet Works</i></b></p> <p><b>Josh Goldfoot</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>(CHIPS ONLY)</b></p>
<p><b>3:00 p.m. - 4:00 p.m.</b></p>	<p><b><i>Obtaining Stored Communications and Records</i></b></p> <p><b>Josh Goldfoot</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>(CHIPS ONLY)</b></p>
	<p><b><i>A CHIP's Guide to Industry Outreach and Case Development</i></b></p> <p><b>Michael L. Levy</b>, Chief Computer Crimes, Assistant U.S.</p>

4:00 p.m. - 5:00 p.m.	<p>Attorney, Eastern District of Pennsylvania, U.S. Department of Justice, Philadelphia, Pennsylvania</p> <p><b>Matthew J. Bassiur</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>Moderated by: Robin Taylor</b>, Computer Hacking and Intellectual Property (CHIP) Program Coordinator, Assistant U.S. Attorney, Eastern District of California, Sacramento, California</p> <p><b>(CHIPS ONLY)</b></p>
-----------------------	---

\*All times and speakers are tentative and are subject to change.

\*\*Pre-register for the Intermediate Control Systems Security training session by sending an email to [gfirst@us-cert.gov](mailto:gfirst@us-cert.gov).

**2008 GFIRST NATIONAL CONFERENCE  
ORLANDO, FLORIDA | JUNE 1-6, 2008**

**Uniting the Cyber Response Community**

**AGENDA**

<b>Tuesday, June 3*</b>	
7:00 a.m. - 5:00 p.m.	<b>Registration Open</b>
8:00 a.m. - 8:30 a.m.	<p><b>Opening Session / Welcome</b></p> <p><b>National Cyber Security Division, U.S. Department of Homeland Security / U.S. Department of Justice / InfraGard</b></p> <p><b>Robert D. Jamison</b>, Under Secretary for National Protection and Programs Directorate, U.S. Department of Homeland Security</p>
8:30 a.m. - 10:00 a.m.	<p><b>Plenary Session</b></p> <p><i>Will There Be Any Security in a Web-Services World?</i></p> <p><b>Dr. Whitfield Diffie</b>, Vice President &amp; Chief Security Officer, Sun Microsystems</p>
10:00 a.m. - 10:30 a.m.	<b>Morning Break</b>
	<b>MANAGEMENT TRACK</b>



10:30 a.m. - 11:15 a.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Today's Threat Landscape and Crimeware's Modular Code</i></p> <p><b>Dean Turner</b>, Director, Global Intelligence Network, Symantec Corporation, Cupertino, California</p>
11:30 a.m. - 12:15 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Evolving Cyber Threat Creates Incident Management Challenges</i></p> <p><b>Jeanie M. Larson</b>, Federal Program Manager, U.S. Department of Energy</p>
12:15 p.m. - 1:15 p.m.	<p><b>Lunchtime Presentation</b></p> <p><i>Real Experiences in Law Enforcement, Government, Military and Private Sector: The Trust and Relationships that Drive True Partnership - Panel</i></p> <p><b>Dr. Kathleen Kiernan</b>, CEO, Kiernan Group</p> <p><b>Raymond F. Geoffroy</b>, Assistant Deputy Commandant, Plans, Policies and Operations (Security) Headquarters, U.S. Marine Corps</p> <p><b>William Casey</b>, Deputy Superintendent, Boston Police Department and Commanding Officer of the Information Technology Division</p> <p><b>Shawn Henry</b>, Deputy Assistant Director, FBI Cyber Division</p> <p><b>Michael Hershman</b>, President, The Fairfax Group</p> <p><b>Ronald Dick</b>, Director, Homeland Security Programs, Computer Sciences Corporation</p> <p><b>Sue Mencer</b>, Policy Director, Brownstein Hyatt Farber &amp; Schreck, LLP</p> <p><b>Moderated by: Dr. Phyllis A. Schneck</b>, Chairman, Board of Directors, InfraGard National Members Alliance and VP, Research Integration, Secure Computing Corporation</p>
1:30 p.m. - 2:15 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Public and Private Collaboration for Improved National Cyber Security</i></p> <p><b>Peter Allor</b>, Director of Intelligence, IBM Global Technology Services, Internet Security Systems</p>
2:15 p.m. - 3:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Driving Security in Software</i></p>

	<p><b>Elliot Glazer</b>, Director of Security Architect, The Depository Trust &amp; Clearing Corporation (DTCC)</p>
1:30 p.m. - 2:15 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>Today's Threats and Why They Are Evading Your Current Detection Infrastructures</i></p> <p><b>Amit Yoran</b>, CEO, NetWitness Corporation</p>
2:15 p.m. - 3:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>Using Logs for Incident Response and Forensics</i></p> <p><b>Dr. Anton Chuvakin</b>, Chief Logging Evangelist, LogLogic</p>
1:30 p.m. - 2:30 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Lam on the Lam: How to Find, Arrest and Prosecute International Suppliers and Importers of Counterfeit Goods without Letting Them Get Away</i></p> <p><b>Brian R. Hood</b>, Assistant U.S. Attorney, Eastern District of Virginia, U.S. Department of Justice, Richmond, Virginia</p> <p><b>John H. Zacharia</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
2:30 p.m. - 3:45 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>CAN-SPAM and Beyond: Perspectives from Recent Prosecutions - Panel</i></p> <p><b>Thomas G. A. Brown</b>, Assistant U.S. Attorney, Southern District of New York, U.S. Department of Justice, New York, New York</p> <p><b>Terrance G. Berg</b>, First Assistant U.S. Attorney, Eastern District of Michigan, U.S. Department of Justice, Detroit, Michigan</p> <p><b>Mona S. Spivack</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>Kathryn A. Warma</b>, Assistant U.S. Attorney, Western District of Washington, U.S. Department of Justice, Seattle, Washington</p> <p><b>Moderated by: Thomas Dukes</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
1:30 p.m. - 2:15 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Incident Response and Network Forensics: Avoiding Common IR Errors</i></p>

	<p><b>Harold Stonebraker</b>, Senior Security Analyst, CISSP, FireEye, Inc.</p>
2:15 p.m. - 3:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Live Memory Acquisition and Analysis</i></p> <p><b>Cal Waits</b>, Member of the Technical Staff, CERT Coordination Center</p>
3:00 p.m. - 3:15 p.m.	<p><b>Afternoon Break</b></p>
3:15 p.m. - 4:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Understanding What Really Happens to Identities Following a Data Breach</i></p> <p><b>Thomas Oscherwitz</b>, Vice President of Government, ID Analytics, Inc.</p>
4:15 p.m. - 5:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>The National Response Framework (NRF) - What Every Business Should Know</i></p> <p><b>Robert Janusaitis</b>, President, Business911 International, Inc.</p>
3:15 p.m. - 4:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>ActiveX Fuzzing with Dranzer: One Thousand Vulnerabilities Later</i></p> <p><b>Will Dormann</b>, Vulnerability Analyst, CERT Coordination Center</p>
4:15 p.m. - 5:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>Network Artifact Analysis</i></p> <p><b>Aaron Hackworth</b>, Senior Member of Technical Staff, CERT Coordination Center</p> <p><b>(Closed Session: Only Federal Employees and/ or Contractors)</b></p>
4:00 p.m. - 5:15 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Cracking the Iceman: A Case Study in Tackling Encryption and Other Problems Associated with Searching Sophisticated Targets</i></p> <p><b>Matt Geiger</b>, Forensic Specialist and Researcher, Computer Emergency Response Team Coordination Center (CERT), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania</p> <p><b>Rich Nolan</b>, Technical Staff, Computer Emergency Response Team Coordination Center (CERT), Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania</p>

	<p><b>Christian Roylo</b>, Special Agent, U.S. Secret Service, U.S. Department of Homeland Security, Pittsburgh, Pennsylvania</p> <p><b>Moderated by: Luke E. Dembosky</b>, Assistant U.S. Attorney, Western District of Pennsylvania, U.S. Department of Justice, Pittsburgh, Pennsylvania</p>
3:15 p.m. - 4:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Dramatically Accelerating Incident Response and Zero Day Exploit Identification</i></p> <p><b>Edward Schwartz</b>, Chief Security Officer, NetWitness Corporation</p>
4:15 p.m. - 5:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>GPS Forensics</i></p> <p><b>Malcolm Smith</b>, Forensic Track Manager, Defense Cyber Investigations Training Academy</p>

\*All times and speakers are tentative and are subject to change.

**2008 GFIRST NATIONAL CONFERENCE**  
**ORLANDO, FLORIDA | JUNE 1–6, 2008**

**Uniting the Cyber Response Community**

**AGENDA**

<b>Wednesday, June 4*</b>	
7:00 a.m. - 5:00 p.m.	<b>Registration Open</b>
8:30 a.m. - 10:00 a.m.	<p><b>Plenary Session</b></p> <p><i>Has Pakistan Stolen Your Traffic Lately? - Threats to Internet Routing and Global Connectivity</i></p> <p><b>Earl Zmijewski, Ph.D</b>, Vice President and General Manager of Internet Data Services, Renesys Corporation</p>
10:00 a.m. - 10:30 a.m.	<b>Morning Break</b>
10:30 a.m. - 11:15 a.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Preparing for the Unpredictable Event</i></p> <p><b>Eric Cowperthwaite</b>, Chief Information Security Officer, Providence Health &amp; Services</p>
	<b>MANAGEMENT TRACK</b>

<p>11:30 a.m. - 12:15 p.m.</p>	<p><b><i>Using Incident Trend Analysis to Reduce CIRT Man-Hours</i></b></p> <p><b>Jack Gabriel</b>, Auditing &amp; Monitoring Team, Federal Trade Commission</p> <p><b>Chris DiGiamo</b>, Lead Analyst, Federal Trade Commission</p> <p><b>Phillip Kealy</b>, Lead Analyst, Federal Trade Commission</p>
<p>10:30 a.m. - 11:15 a.m.</p>	<p><b>TECHNICAL TRACK</b></p> <p><b><i>Control System Cyber Incident Handling: A Law Enforcement Perspective - Panel</i></b></p> <p><b>David Black</b>, CISM, Acting Director, Technical Security Branch, RCMP</p> <p><b>Jeff Morgan</b>, Process Control Systems Analyst, FBI Cyber Crime Division</p> <p><b>Scott Aken</b>, Special Agent, FBI, Computer Intrusion and Cyber Action Team</p> <p><b>Christian Roylo</b>, Special Agent, U.S. Secret Service, U.S. Department of Homeland Security, Pittsburgh, Pennsylvania</p> <p><b>Moderated by:</b> <b>Mark Fabro</b>, CISSP, CISM, President and CEO, Lofty Perch, Inc.</p>
<p>11:30 a.m. - 12:15 p.m.</p>	<p><b>TECHNICAL TRACK</b></p> <p><b><i>Identity Monitoring</i></b></p> <p><b>Colby DeRodeff</b>, Enterprise Solutions Strategist, ArcSight, Inc.</p> <p><b>Brian T. Contos</b>, CISSP, Chief Security Officer, ArcSight, Inc.</p>
<p>10:30 a.m. - 11:30 a.m.</p>	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><b><i>Obtaining Electronic Evidence Series: Google Update - Today and Tomorrow</i></b></p> <p><b>Cathy A. McGoff</b>, Senior Manager, Online Operations Legal Support, Google, Inc., Mountain View, California</p> <p><b>Marc S. Crandall</b>, Product Counsel, Legal Department, Google, Inc., Mountain View, California</p> <p><b>Moderated by:</b> <b>Richard Downing</b>, Assistant Deputy Chief for Computer Crime Technology Policy, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
	<p><b>LAW ENFORCEMENT TRACK</b></p>

11:30 a.m. - 12:15 p.m.	<p><b><i>Practical Considerations When You Learn Your Defendant Hacker and IP Violator is a Juvenile</i></b></p> <p><b>Mark Krause</b>, Assistant U.S Attorney, Central District of California, U.S. Department of Justice, Los Angeles, California</p> <p><b>Stephen P. Heymann</b>, Chief, Computer Crime Unit, District of Massachusetts, U.S. Department of Justice, Boston, Massachusetts</p>
10:30 a.m. - 11:15 a.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><b><i>Lessons From Defending Cyberspace</i></b></p> <p><b>Robert B. Dix, Jr.</b>, Vice President of Government Affairs, Juniper Networks</p>
11:30 a.m. - 12:15 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><b><i>Framework for Responding to Network System Events: Autonomic, Policy-based Response</i></b></p> <p><b>Scott Miller</b>, ACS-PO Senior System Architect, Los Alamos National Laboratory</p>
12:15 p.m. - 1:15 p.m.	<p><b>Lunchtime Presentation</b></p> <p><b><i>DHS Cyber Exercise Program, Cyber Storm: The Importance of Building and Exercising Partnerships and Stakeholder Collaboration</i></b></p> <p><b>Brett M. Lambo</b>, Director, Cyber Exercise Program, National Cyber Security Division, U.S. Department of Homeland Security</p>
1:30 p.m. - 2:15 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><b><i>Building an Effective Communications Framework: Goals, Objectives, and Strategies</i></b></p> <p><b>Mr. Leonard Luterbach</b>, Program and Policy Analyst, Office of the Comptroller of the Currency, U.S. Department of Treasury</p>
2:15 p.m. - 3:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><b><i>Reinventing FISMA - Finding the Right Metrics to Measure Government Program Success</i></b></p> <p><b>Mischel Kwon</b>, Chief Security Technologist, U.S. Department of Justice</p> <p><b>Rich Marshall</b>,</p> <p><b>Amit Yoran</b>, CEO, NetWitness Corporation</p> <p><b>Sean McAllister</b>, Chief, Enterprise Sensor Grid Management Branch, Defense Information Systems Agency (DISA)</p>

1:30 p.m. - 2:15 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>MSRC - How Microsoft Responds to Vulnerabilities and the Processes It Uses, From Responsible Disclosure to Zero-day Threats</i></p> <p><b>Zot O'Conner</b>, Senior Security Strategist, Microsoft Security Response Center</p>
2:15 p.m. - 3:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>The Role of Internet Reputation Intelligence in Critical Infrastructure Protection</i></p> <p><b>Dr. Phyllis A. Schneck</b>, Chairman, Board of Directors, InfraGard National Members Alliance and VP, Research Integration, Secure Computing Corporation</p>
1:30 p.m. - 2:30 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Forensic Issues Related to Microsoft Vista, Encryption, and Volatile Data</i></p> <p><b>Ovie L. Carroll</b>, Chief, Cybercrime Lab, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
2:30 p.m. - 3:30 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Judicial Trends, Developments in the Law of Electronic Evidence</i></p> <p><b>Howard W. Cox</b>, Assistant Deputy Chief, Computer Crime Litigation, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
1:30 p.m. - 2:15 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>OPS-Reach: Aligning Outreach Activities to Support the Operational Mission - Panel</i></p> <p>TBA</p>
2:15 p.m. - 3:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>The Latest Malware Techniques</i></p> <p><b>Greg Feezel</b>, Director, Information Security, Snap-on Business Solutions</p> <p><b>Tyler Hudak</b>, Senior Security Consultant, KoreLogic Security</p>
3:00 p.m. - 3:15 p.m.	<p><b>Afternoon Break</b></p>
3:15 p.m. - 4:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Architecting Security Measurement &amp; Management for Compliance</i></p>

	<p><b>Robert A. Martin</b>, Principle Engineer, The MITRE Corporation</p>
4:15 p.m. - 5:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Software Assurance: Mitigating Risks to the Enterprise - Panel</i></p> <p><b>Moderated by: Joe Jarzombek</b>, Director for Software Assurance, National Cyber Security Division, U.S. Department of Homeland Security</p>
3:15 p.m. - 4:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>How Software and Hardware Vendors Respond to Threats and Vulnerabilities - Panel</i></p> <p><b>Peter Allor</b>, Program Manager for Intelligence and Vendor Relations, IBM Internet Security Systems</p> <p><b>Zot O'Conner</b>, Senior Security Strategist, Microsoft Security Response Center</p> <p><b>Bernie Rosen</b>, Director, Security Incident Response Team, Juniper Networks</p> <p><b>Bill Taub</b>, Vice President, Enterprise Security, CA</p> <p><b>Moderated by: Scott Algeier</b>, Executive Director, IT-ISAC</p>
4:15 p.m. - 5:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>Creating an Operational Tempo with US-CERT Information Products</i></p> <p><b>Mark William Henderson</b>, Senior Analyst, General Dynamics Advanced Information Systems</p> <p><b>(Closed Session: Only Federal Employees and/ or Contractors)</b></p>
3:45 p.m. - 5:15 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Obtaining Evidence Abroad: Overcoming International Challenges - Panel</i></p> <p><b>Gavin A. Corn</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>Christopher P. Sonderby</b>, Attaché for the U.S. Department of Justice, Intellectual Property Law Enforcement Coordinator (IPLEC) for Asia, U.S. Department of Justice, U.S. Embassy in Bangkok, Bangkok, Thailand</p> <p><b>Matthew A. Lamberti</b>, Intellectual Property Law Enforcement Coordinator (IPLEC) for Eastern Europe, U.S. Department of Justice, U.S. Embassy in Sofia, Sofia,</p>

	<p>Bulgaria</p> <p><b>Dan Valentin Fatuloiu</b>, Minister-Counselor, Embassy of Romania, Washington, DC</p> <p><b>Kimberly Kiefer Peretti</b>, Senior Counsel, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>Moderated by: Betty Shave</b>, Assistant Deputy Chief, International Computer Crime, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
3:15 p.m. - 4:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Advancing Internal Network Security: Beyond Perimeter and Host Protection</i></p> <p><b>Joshua Corman</b>, Principle Security Strategist, IBM Internet Security Systems, IBM Global Technology Services</p> <p><i>How Software and Hardware Vendors Respond to Threats and Vulnerabilities</i></p> <p>TBD</p>
4:15 p.m. - 5:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Protecting U.S. Cyberspace: Coordinating a National Response to Cyber Attacks</i></p> <p><b>Brett Lambo</b>, Director, Cyber Exercise Program, National Cyber Security Division, U.S. Department of Homeland Security</p> <p><b>Christopher Painter</b>, Senior Counsel to the Assistant Attorney General, U.S. Department of Justice</p> <p><b>Anthony Bargar</b>, Senior Policy and Strategy Advisor, Deputy Assistant Secretary of Defense for Information and Identity Assurance</p>
6:00 p.m.	<p><b>Birds-of-a-Feather</b></p> <p><i>US-CERT</i></p> <p>(Closed Session: Only Federal Employees and/ or Contractors)</p>
6:00 p.m.	<p><b>Birds-of-a-Feather</b></p> <p><i>DNS Server Protection</i></p> <p><b>Moderated by: Donald A. Purdy, Jr., Esq.</b>, CISSP, Executive Advisory Board of BigFix, Inc., Partner, Allenbaugh Samini, LLP</p> <p><b>Moderated by: Arun Sood</b>, Professor, Computer</p>

	Science, George Mason University
6:00 p.m.	<b>Birds-of-a-Feather</b>

\*All times and speakers are tentative and are subject to change.

**2008 GFIRST NATIONAL CONFERENCE**  
**ORLANDO, FLORIDA | JUNE 1-6, 2008**

**Uniting the Cyber Response Community**

**AGENDA**

<b>Thursday, June 5*</b>	
7:00 a.m. - 5:00 p.m.	<b>Registration Open</b>
8:30 a.m. - 10:00 a.m.	<b>Plenary Session</b> <i>They Didn't Really Do That, Did They?</i> <b>Rick Estberg</b> , Chief of Staff, Interagency OPSEC Support Staff, U.S. Department of Defense
10:00 a.m. - 10:30 a.m.	<b>Morning Break</b>
10:30 a.m. - 11:15 a.m.	<b>MANAGEMENT TRACK</b> <i>Improving the Cyber Security of the Nation's Critical Infrastructure and Key Resources</i> <b>Jenny Menna</b> , Director, CIP, National Cyber Security Division, U.S. Department of Homeland Security
11:30 a.m. - 12:15 p.m.	<b>MANAGEMENT TRACK</b> <i>New Horizons for Control Systems Security</i> <b>Sean McGurk</b> , Director, Control Systems Security Program, U.S. Department of Homeland Security
10:30 a.m. - 11:15 a.m.	<b>TECHNICAL TRACK</b> <i>JavaScript and DHTML Malware - The Emerging Threat</i> <b>Robert Hansen</b> , CEO, SecTheory, LLC
11:30 a.m. - 12:15 p.m.	<b>TECHNICAL TRACK</b> <i>Typo Squatting: One Keystroke Away from Doom</i>

	<p><b>Adam Meyers</b>, Principle, SRA International</p>
10:30 a.m. - 11:30 a.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>View From The Bench: Cyber and IP Crimes - Panel</i></p> <p><b>The Honorable Ronald S. W. Lew</b>, Judge of the United States District Court, Central District of California, Los Angeles, California</p> <p><b>The Honorable Jeremy Fogel</b>, Judge of the United States District Court, Northern District of California, San Jose, California</p> <p><b>Moderated by: Matthew J. Bassiur</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
11:30 a.m. - 12:15 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Computer Forensics - Initially Get What Your Really Need: Prosecution Initial Request List (PIRL) Presentation and Update - Panel</i></p> <p><b>Timothy M. O'Shea</b>, Senior Litigation Counsel, Western District of Wisconsin, U.S. Department of Justice, Madison, Wisconsin</p> <p><b>Michael L. Levy</b>, Chief of Computer Crimes, Assistant U.S. Attorney, Eastern District of Pennsylvania, U.S. Department of Justice, Philadelphia, Pennsylvania</p> <p><b>Arnold H. Huftalen</b>, Assistant U.S. Attorney, District of New Hampshire, U.S. Department of Justice, Concord, New Hampshire</p> <p><b>Stephen P. Heymann</b>, Chief, Computer Crime Unit, District of Massachusetts, U.S. Department of Justice, Boston, Massachusetts</p> <p><b>Dan L. Newsom</b>, Senior Litigation Counsel, Western District of Tennessee, U.S. Department of Justice, Memphis, Tennessee</p> <p><b>Ovie L. Carroll</b>, Chief, Cybercrime Lab, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p> <p><b>Moderated by: Martin J. Littlefield</b>, Senior Litigation Counsel, Western District of New York, U.S. Department of Justice, Buffalo, New York</p>
10:30 a.m. - 11:15 a.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Threats to the 2008 Presidential Election</i></p> <p><b>Oliver Friedrichs</b>, Director, Emerging Technologies, Symantec Corporation</p>
	<p><b>INCIDENT RESPONSE TRACK</b></p>

11:30 a.m. - 12:15 p.m.	<p><b><i>Intrusion Tolerance - An Approach for Proactive Risk Management</i></b></p> <p><b>Arun Sood</b>, Professor, Computer Science, George Mason University</p>
12:15 p.m. - 1:15 p.m.	<p><b>Lunchtime Presentation</b></p> <p><b><i>Connecting the Cybersecurity Players - Panel</i></b></p> <p><b>Dean Turner</b>, Director, Global Intelligence Network, Symantec Corporation, Cupertino, California</p> <p><b>Mike Russo</b>, Chief Information Security Officer for the State of Florida, Tallahassee, Florida</p> <p><b>Donna M. Peterson</b>, Acting Assistant Section Chief, FBI, U.S. Department of Justice, Washington, DC</p> <p><b>John M. Bodenhausen</b>, Assistant U.S. Attorney, Eastern District of Missouri, U.S. Department of Justice, St. Louis, Missouri</p> <p><b>Moderated by: Howard W. Cox</b>, Assistant Deputy Chief, Computer Crime Litigation, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
1:30 p.m. - 2:15 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><b><i>Enterprise-Grade Incident Management: Responding to the Persistent Threat</i></b></p> <p><b>Sunil James</b>, Director of Product Management, MANDIANT</p> <p><b>David Ross</b>, Principal Consultant, MANDIANT</p>
2:15 p.m. - 3:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><b><i>Cyber Event Response Places Your Mission at Risk</i></b></p> <p><b>Peter Gouldmann</b>, Security Architect, U.S. Department of State</p>
1:30 p.m. - 3:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><b><i>BitTorrent: The Swarm of Internet Crime</i></b></p> <p><b>Brian Baskin</b>, Deputy Technical Lead, Cyber Crime Center, U.S. Department of Defense</p>
1:30 p.m. - 2:45 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><b>(Closed Session: CHIPS ONLY)</b></p>
1:30 p.m. - 2:15 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><b><i>Volatile and Memory Analysis in a Network Environment</i></b></p>

	<p><b>Christopher J. Mellen</b>, Director of Professional Services, AccessData, Inc.</p>
2:15 p.m. - 3:00 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Advanced Persistent Threat</i></p> <p><b>Ryan Walters</b>, Director of Security Solutions, Northrop Grumman Corporation</p>
3:00 p.m. - 3:15 p.m.	<p><b>Afternoon Break</b></p>
3:15 p.m. - 4:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Web 2.0 Meets Security 2.0</i></p> <p><b>John McCumber</b>, Strategic Programs Manager, Symantec Corporation</p>
4:15 p.m. - 5:00 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><i>Incident Handling Lifecycle - Detection, Assessment, Validation, Reporting, and Post-Incident Analysis</i></p> <p><b>Mauricio Angee</b>, Senior Information Security Systems, Harris Corporation</p>
3:15 p.m. - 5:00 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><i>Building a Custom Log Analysis Platform for Incident Response</i></p> <p><b>Edward Collins</b>, Manager, CIAN, Inc.</p>
2:45 p.m. - 3:45 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p>(Closed Session: CHIPS ONLY)</p>
4:00 p.m. - 5:15 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Economic Espionage Act and Trade Secret Prosecutions: Overcoming The Challenges - Panel</i></p> <p><b>Lawrence E. Kole</b>, Senior Litigation Counsel, Central District of California, U.S. Department of Justice, Santa Ana, California</p> <p><b>Randy S. Chartash</b>, Chief, Economic Crime Section, Northern District of Georgia, U.S. Department of Justice, Atlanta, Georgia</p> <p><b>Moderated by: Mark L. Krotoski</b>, National Computer Hacking and Intellectual Property (CHIP) Program Coordinator, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Malware Analysis: The Forgotten Forensic Skill</i></p>

<p>3:15 p.m. - 4:00 p.m.</p>	<p><b>Greg Feezel</b>, Director, Information Security, Snap-on Business Solutions</p> <p><b>Tyler Hudak</b>, Senior Security Consultant, KoreLogic Security</p>
<p>4:15 p.m. - 5:00 p.m.</p>	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>The Complexity of Managing Government Network Security</i></p> <p><b>Gregory Jones</b>, Senior Security Manager, Northrop Grumman Corporation</p>
<p>6:00 p.m.</p>	<p><b>Birds-of-a-Feather</b></p> <p><i>What's Coming Down the Pike? A Discussion of IP and Other High-Tech Legal Issues on the Horizon (Or Just Over It)</i></p> <p><b>Jason Gull</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
<p>6:00 p.m.</p>	<p><b>Birds-of-a-Feather</b></p> <p><i>Cyber Swat Teams: "Specialists with Automated Tools" Leveraging Collaboration to Achieve Security Priorities</i></p> <p>Moderated by: Dennis Heretick</p>
<p>6:00 p.m.</p>	<p><b>Birds-of-a-Feather</b></p> <p><i>SANS Internet Storm Center</i></p> <p>Moderated by: <b>Marcus Sachs</b>, Director, SANS Internet Storm Center</p>

\*All times and speakers are tentative and are subject to change.

**2008 GFIRST NATIONAL CONFERENCE**  
**ORLANDO, FLORIDA | JUNE 1–6, 2008**

**Uniting the Cyber Response Community**

**AGENDA**

<p>Friday, June 6*</p>	
<p>8:00 a.m. - 12:00 p.m.</p>	<p>Registration Open</p>
	<p>Plenary Session</p>

8:30 a.m. - 10:00 a.m.	<p><b><i>Large Scale Data Breaches: Taking Numbers Off the Street</i></b></p> <p><b>Edward Lowery</b>, Assistant Special Agent in Charge, Criminal Investigatory Division, U.S. Secret Service, U.S. Department of Homeland Security, Washington, DC</p> <p><b>Andrew Valentine</b>, Senior Consultant, Investigative Response, Cybertrust / Verizon Business, Dallas, Texas</p> <p><b>Ingrid Beierly</b>, Director, Cardholder Information Security Program, Cyber Security and Investigations, Visa, Inc., Foster City, California</p> <p><b>Moderated by: Kimberly Kiefer Peretti</b>, Senior Counsel, Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice, Washington, DC</p>
10:00 a.m. - 10:30 a.m.	<b>Morning Break</b>
10:30 a.m. - 11:15 a.m.	<p><b>MANAGEMENT TRACK</b></p> <p><b><i>Mega to Microscopic IT Risk Assessment and Response</i></b></p> <p><b>Julian Waits</b>, President &amp; CEO, Brabeion Software</p>
11:30 a.m. - 12:15 p.m.	<p><b>MANAGEMENT TRACK</b></p> <p><b><i>Implementing Effective Vulnerability and Threat Management</i></b></p> <p><b>Amrit Williams</b>, Chief Technology Officer, BigFix, Inc.</p>
10:30 a.m. - 11:15 a.m.	<p><b>TECHNICAL TRACK</b></p> <p><b><i>Design Choices in Creating a Malware Laboratory</i></b></p> <p><b>Grant Deffenbaugh</b>, Member of Technical Staff, CERT Coordination Center</p>
11:30 a.m. - 12:15 p.m.	<p><b>TECHNICAL TRACK</b></p> <p><b><i>The State of Rootkits and Virtualization</i></b></p> <p><b>David Marcus</b>, Security Research Manager, McAfee (Avert Labs)</p>
10:30 a.m. - 11:15 a.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><b><i>Using All The Tools: Copyright Infringement, WiFi Theft, Mail Fraud and ID Theft</i></b></p> <p><b>Marc Miller</b>, Trial Attorney, Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice, Washington, DC</p> <p><b>Michael Godfrey</b>, Senior Special Agent, Cyber Crimes Center, U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security, Fairfax, Virginia</p>

11:15 a.m. - 12:15 p.m.	<p><b>LAW ENFORCEMENT TRACK</b></p> <p><i>Hot Ethical Topics in Cybercrime: Taint Teams and Contacts with Represented Parties</i></p> <p><b>Eric Klumb</b>, Assistant U.S. Attorney, District of South Carolina, U.S. Department of Justice, Charleston, South Carolina</p>
10:30 a.m. - 11:15 a.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Five Common Mistakes in Securing Web Applications</i></p> <p><b>John Weinschenk</b>, CEO &amp; President, Cenzic, Inc.</p>
11:30 a.m. - 12:15 p.m.	<p><b>INCIDENT RESPONSE TRACK</b></p> <p><i>Application Whitelisting: Information Assurance and Desktop Lockdown</i></p> <p><b>Tom Murphy</b>, Chief Strategist, Bit9, Inc.</p>
12:15 p.m. - 1:15 p.m.	<p><b>Closing Program</b></p>

\*All times and speakers are tentative and are subject to change.