



Lessons Learned Information Sharing

www.LLIS.gov

SHARING INFORMATION
ENHANCING PREPAREDNESS
STRENGTHENING HOMELAND SECURITY

LLIS.gov Resources for Cyber Security Preparedness

A TOOL FOR ENHANCING NATIONAL PREPAREDNESS

Lessons Learned Information Sharing (LLIS.gov) is a US Department of Homeland Security/Federal Emergency Management Agency program. *LLIS.gov* serves as the national, online network of lessons learned, best practices, and innovative ideas for the emergency response and homeland security communities. This information and collaboration resource helps emergency response providers and homeland security officials prevent, protect against, respond to, and recover from terrorist attacks, natural disasters, and other emergencies. *LLIS.gov* provides Federal, State, and local responders with a wealth of information and front-line expertise on effective planning, training, and operational practices across homeland security functional areas.

LLIS.gov at a Glance

- Online since April 19, 2004
- Over 43,000 registered members
- Over 12,000 documents, including more than 1,500 state and local plans, 600 after-action reports, and 750 original content documents
- Secure message boards and collaboration tools
- Targeted information on current homeland security topics

Cyber Security

America's cyber infrastructure is vulnerable to attack because organizations face an ever growing set of adversaries, intent on creating new, hard to detect exploits that are difficult to defend against. With the cyber infrastructure underpinning the physical infrastructure, homeland security personnel from all organizations—law enforcement, emergency management, public health, public works, information technology, intelligence fusion centers—need to consider and address cyber security implications within the aspects of their work.

Incidents around the globe highlight the unique challenges cyber responders and homeland security officials and their private sector partners face when trying to secure the cyber infrastructure. The increasing number of incidents demonstrates the need for continued security planning and preparation in the United States. To this end, LLIS.gov has partnered with the Department of Homeland Security's (DHS) National Cyber Security Division (NCS) to provide emergency planners with a single source to start their cyber security research and planning. LLIS.gov also offers a discussion forum and feedback tool to enhance planning and collaboration initiatives among homeland security personnel from all organizations. Additional sites managed by the National Cyber Security Division/Cyber Security Operations Team (US-CERT) and the Public-Private Information Sharing and Analysis Center (PPISAC) may also be of use to LLIS.gov members.

The NCS/DHS-CERT wants to ensure that Americans have the information they need to secure their portion of cyber space. DHS is committed to continuing and enhancing collaborative efforts with the private and public sectors to raise the awareness of cyber security for all computer users and reduce cyber risk. The *National Cyber Security Division* offers a variety of information for users with varied technical expertise including Technical Cyber Security Alerts and Bulletins, or more general interest areas such as Cyber Security Alerts and Tips on a variety of cyber-related topics. All of these products will assist you and your organization by keeping you informed and up-to-date. US-CERT also maintains a S&C/T Secure Operations Center to provide real-time monitoring of cyber events. One way your organization can help is to report cyber security incidents (including one-paged network failures), the discovery of malicious code, and vulnerability information to US-CERT at submit@us-cert.gov (888) 282-0870, or at www.us-cert.gov.

LLIS.gov needs your help. Active feedback and input from our members enables LLIS.gov's continued expansion and helps us meet the ever-changing needs of the emergency response community. Please take time to improve your community: submit After-Action Reports, Practice Notes, Lessons Learned, plans, templates, strategies, and other relevant information:

- Submit Lessons Learned and Innovative Practices
- Submit Plans, After-Action Reports, and Other Documents
- Email Comments, Experiences, and Observations

<p>CYBER SECURITY RESOURCE LIBRARY</p> <p>Policy Guidance</p> <ul style="list-style-type: none"> National Response Framework National Response Framework, EOP #2 - Communications Annex National Response Framework, Cyber Incident Annex IRFA 1000 - Standard on Incident Response Management and Business Continuity, Version 3.00 - Edition <p>View All Policy Guidance</p> <p>Cyber Security Planning</p> <ul style="list-style-type: none"> 2008 Industry Outlook: A Look Around the Corner - U.S. Federal & State Agencies Continuity of Operations (COOP) Planning Guidelines for 	<p>DHS National Cyber Security Division</p> <ul style="list-style-type: none"> National Strategy to Secure Cyber Space <ul style="list-style-type: none"> Cyber Security 101 Briefing Presentation (PowerPoint) Information for Reporting Cyber Incidents US-CERT Products and Capabilities Cyber Security Preparedness Other <ul style="list-style-type: none"> Control Systems Security Program Exports and Tools US Computer Emergency Readiness Team US Central System Security Program US Cyber Security Software Assurance and Store National Cyber Security Division Cyber Security Exercise Program
---	---

A RESOURCE FOR ENHANCING CYBER SECURITY

The *LLIS.gov* Cyber Security page is a one-stop resource for information related to improving cyber security preparedness and response planning for government agencies and their homeland security partners. Examples of *LLIS.gov* resources include:

- The National Strategy to Secure Cyberspace
- CYBER STORM I National Exercise After Action Report
- Creating a Cyber Security Incident Response Team (CIRT)
- FY 2007 HSGP Supplemental Resource: Cyber Security Grant Guidance
- Blue Cascades Exercise Series After Action Reports

CYBER SECURITY PLANS, GUIDELINES, AND REPORTS

LLIS.gov's Cyber Security page includes guidance for building cyber security capabilities and for considering how cyber security best practices integrate into existing physical security plans, procedures, and all phases of emergency management, such as:

- Cyber Security 101: An Introductory Briefing for Homeland Security Practitioners
- A Guidebook for Local Government Cyber Security - Getting Started
- Cyber Security Training Opportunities for Law Enforcement Agencies
- 2007 National Cyber Security Awareness Month Tool Kit
- US-CERT Analytic Reports on Cyber Threats
- Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats
- Electronic Social Engineering Exploitation Poses Continuing Threat in Cyberspace
- Risk Assessment: Information Technology & Telecommunications
- Potential Terrorist Threat to the U.S. Information Infrastructure
- Computer Security Incident Handling Guide
- Getting Down to Business – Business Executives for National Security Report

For more information on *LLIS.gov* or to register, please go to www.llis.gov.

LLIS.gov is a Department of Homeland Security/Federal Emergency Management Agency program and is supported by the NxT. For more information, please contact the *LLIS.gov* Help Desk at 866.276.7001 or Feedback@llis.dhs.gov.