

EHS NEWS

*The Environmental,
Health & Safety
Newsletter
from Ergon*

*An Information Bulletin for
Ergon, Inc. and Affiliated
Companies*



Ergon Security at Work and Home

In the November 1, 2005, issue of the EHS News, we mentioned the EHS Department would be offering an audit qualifications program for new facility security auditors in February 2006. These efforts were in response to requests to develop this internal program and represent our continued commitment to the core value of offering the best in customer service. A

Security Auditor Training session was held on February 15-17 at a regionally centered location in Nashville, TN, to accommodate participants' scheduling availability. The desired end-state of the training was to develop auditors who could conduct internal annual security audits as required by the United States Coast Guard (USCG) and by the Maritime Transportation

Protect Your Workplace

Physical Security Guidance



- Monitor and control who is entering your workplace: current employees, former employees, and commercial delivery and service personnel.
- Check identification and ask individuals to identify the purpose of their visit to your workplace.
- Report broken doors, windows, and locks to your organization's or building's security personnel as soon as possible.
- Make back-ups or copies of sensitive and critical information and databases.
- Store, lock, and inventory your organization's keys, access cards, uniforms, badges, and vehicles.
- Monitor and report suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, garages, and immediate vicinity.
- Report suspicious-looking packages to your local police. **DO NOT OPEN OR TOUCH.**
- Shred or destroy all documents that contain sensitive personal or organizational information that is no longer needed.
- Keep an inventory of your most critical equipment, hardware, and software.
- Store and lock your personal items such as wallets, purses, and identification when not in use.

Call your local police department to report a suspicious person, vehicle, or activity in or near your workplace.

Call 911 if it is an emergency.

To download this poster, visit www.US-CERT.gov



Report Suspicious Behavior and Activity

SURVEILLANCE

Are you aware of anyone recording or monitoring activities, taking notes, using cameras, microphones, binoculars, etc., near a key facility?

TESTS OF SECURITY

Are you aware of any attempts to penetrate or test physical security or procedures at a key facility?

DEPLOYING ASSETS

Have you observed abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility?

ACQUIRING SUPPLIES

Are you aware of anyone attempting to improperly acquire supplies, weapons, ammunition, dangerous chemicals, uniforms, badges, flight manuals, access cards, or identification for a key facility or to legally obtain items under suspicious circumstances that could be used in a terrorist act?

SUSPICIOUS PERSONS

Are you aware of anyone who does not appear to belong in the workplace, neighborhood, business establishment, or near a key facility?

DRY RUNS

Have you observed any behavior that appears to be preparation for terrorist activities, such as mapping out routes, playing out scenarios with other people, monitoring key facilities, timing traffic lights or traffic flow, or other suspicious activities?

SUSPICIOUS QUESTIONING

Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding a key facility or its operations?

Call 911 if there is an emergency or immediate threat. Call the nearest Joint Terrorism Task Force (JTTF) to report suspicious activity or behavior (see below). Submit information electronically at www.us-cert.gov

Alaska (204) 471-6222	Connecticut (203) 426-6222	Florida (305) 426-6222	Illinois (618) 426-6222	Mississippi (601) 426-6222
Arizona (602) 426-6222	Delaware (302) 426-6222	Georgia (404) 426-6222	Indiana (317) 426-6222	Minnesota (612) 426-6222
Arkansas (501) 426-6222	District of Columbia (202) 426-6222	Hawaii (808) 426-6222	Iowa (319) 426-6222	Montana (406) 426-6222
California (916) 426-6222	Honolulu (808) 426-6222	Idaho (208) 426-6222	Kansas (913) 426-6222	Nebraska (402) 426-6222
Colorado (303) 426-6222	Michigan (313) 426-6222	Kentucky (502) 426-6222	Kentucky (502) 426-6222	Nevada (702) 426-6222
Connecticut (203) 426-6222	Minnesota (612) 426-6222	Louisiana (504) 426-6222	Louisiana (504) 426-6222	New Hampshire (603) 426-6222
Florida (305) 426-6222	Mississippi (601) 426-6222	Maine (207) 426-6222	Maine (207) 426-6222	New Jersey (908) 426-6222
Georgia (404) 426-6222	Michigan (313) 426-6222	Maryland (410) 426-6222	Maryland (410) 426-6222	New Mexico (505) 426-6222
Hawaii (808) 426-6222	Minnesota (612) 426-6222	Massachusetts (617) 426-6222	Massachusetts (617) 426-6222	New York (914) 426-6222
Idaho (208) 426-6222	Missouri (314) 426-6222	North Carolina (919) 426-6222	North Carolina (919) 426-6222	Ohio (614) 426-6222
Illinois (618) 426-6222	Montana (406) 426-6222	North Dakota (701) 426-6222	North Dakota (701) 426-6222	Oklahoma (405) 426-6222
Indiana (317) 426-6222	Nebraska (402) 426-6222	Ohio (614) 426-6222	Ohio (614) 426-6222	Pennsylvania (717) 426-6222
Iowa (319) 426-6222	Nevada (702) 426-6222	Oklahoma (405) 426-6222	Oklahoma (405) 426-6222	Rhode Island (401) 426-6222
Kansas (913) 426-6222	New Hampshire (603) 426-6222	Pennsylvania (717) 426-6222	Pennsylvania (717) 426-6222	South Carolina (803) 426-6222
Kentucky (502) 426-6222	New Jersey (908) 426-6222	South Carolina (803) 426-6222	South Carolina (803) 426-6222	Tennessee (615) 426-6222
Louisiana (504) 426-6222	New Mexico (505) 426-6222	Tennessee (615) 426-6222	Tennessee (615) 426-6222	Texas (214) 426-6222
Maine (207) 426-6222	New York (914) 426-6222	Texas (214) 426-6222	Texas (214) 426-6222	Utah (801) 426-6222
Maryland (410) 426-6222	North Carolina (919) 426-6222	Utah (801) 426-6222	Utah (801) 426-6222	Vermont (802) 426-6222
Massachusetts (617) 426-6222	North Dakota (701) 426-6222	Vermont (802) 426-6222	Vermont (802) 426-6222	Virginia (804) 426-6222
Michigan (313) 426-6222	Ohio (614) 426-6222	Virginia (804) 426-6222	Virginia (804) 426-6222	Washington (206) 426-6222
Minnesota (612) 426-6222	Oklahoma (405) 426-6222	Washington (206) 426-6222	Washington (206) 426-6222	West Virginia (304) 426-6222
Mississippi (601) 426-6222	Pennsylvania (717) 426-6222	West Virginia (304) 426-6222	West Virginia (304) 426-6222	Wisconsin (608) 426-6222
Missouri (314) 426-6222	South Carolina (803) 426-6222	Wisconsin (608) 426-6222	Wisconsin (608) 426-6222	Wyoming (307) 426-6222
Montana (406) 426-6222	Tennessee (615) 426-6222	Wyoming (307) 426-6222	Wyoming (307) 426-6222	
Nebraska (402) 426-6222	Texas (214) 426-6222			
Nevada (702) 426-6222	Utah (801) 426-6222			
New Hampshire (603) 426-6222	Vermont (802) 426-6222			
New Jersey (908) 426-6222	Virginia (804) 426-6222			
New Mexico (505) 426-6222	Washington (206) 426-6222			
New York (914) 426-6222	West Virginia (304) 426-6222			
North Carolina (919) 426-6222	Wisconsin (608) 426-6222			
North Dakota (701) 426-6222	Wyoming (307) 426-6222			
Ohio (614) 426-6222				
Oklahoma (405) 426-6222				
Oregon (503) 426-6222				
Pennsylvania (717) 426-6222				
Rhode Island (401) 426-6222				
South Carolina (803) 426-6222				
South Dakota (605) 426-6222				
Tennessee (615) 426-6222				
Texas (214) 426-6222				
Utah (801) 426-6222				
Vermont (802) 426-6222				
Virginia (804) 426-6222				
Washington (206) 426-6222				
West Virginia (304) 426-6222				
Wisconsin (608) 426-6222				
Wyoming (307) 426-6222				

To download this poster, visit www.us-cert.gov

Report Suspicious Cyber Incidents

SYSTEM FAILURE OR DISRUPTION

Has your system or website's availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

SUSPICIOUS QUESTIONING

Are you aware of anyone attempting to gain information in person, by phone, mail, e-mail, etc., regarding the configuration and/or cyber security posture of your website, network, software, or hardware?

UNAUTHORIZED ACCESS

Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or its data?

UNAUTHORIZED CHANGES OR ADDITIONS

Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent?

SUSPICIOUS E-MAILS

Are you aware of anyone in your organization receiving suspicious e-mails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

UNAUTHORIZED USE

Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

We encourage you to report any activities that you find over the internet for an incident. How do we get help to keep the information specific to your site and system confidential unless we receive your permission to release the information. US-CERT has partnered with law enforcement agencies such as the FBI, Secret Service and the Federal Bureau of Investigation to investigate cyber incidents and prosecute cyber criminals.

Report an incident to the U.S. Computer Emergency Response Team Incident Hotline: 1-888-282-0870 or www.US-CERT.gov

Be even cyber tips, best practices, "how-to" guides, or sign up for technical and non-technical cyber alerts, and to download this poster, visit www.US-CERT.gov



Protect Your Workplace

Cyber Security Guidance



Employees

- Use your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your user names, passwords, or other sensitive website access codes to anyone.
- Do NOT open e-mails or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network or hardware without permission from your IT department.
- Make electronic and physical back-ups or copies of all your most important work.
- Report all suspicious or unusual problems with your computer to your IT department.


Management & IT Department

- Implement Defense in Depth: a layered defense strategy that includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems, and internet content filtering.
- Update your anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.
- Monitor, log, and analyze successful and attempted intrusions to your systems and networks.

Report a computer or network vulnerability to the U.S. Computer Emergency Response Team Incident Hotline: 1-888-282-0870 or www.US-CERT.gov

Be even cyber tips, best practices, "how-to" guides, or sign up for technical and non-technical cyber alerts, and to download this poster, visit www.US-CERT.gov





Security Act of 2002 (MTSA 2002). Ergon EHS performed process mapping sessions to create the audit procedures. So far, these auditors have conducted eleven security audits.

Our Enterprise Security System project is well under way and rapidly nearing completion. So far, numerous CCTV systems, various wireless communication devices, and perimeter defense infrastructure improvements have been implemented at ten Ergon and Lion Oil Company locations. These efforts serve to meet the requirements to reduce security vulnerabilities in the refinery, petrochemical, and maritime industries. They also represent major improvements in our abilities to respond by helping (1) detect, (2) deter, (3) delay, and (4) devalue consequences of potential homeland security threats. Ergon and Lion Oil companies are on the forefront of this effort. The project is scheduled to be completed this fall.

To date, Ergon companies have received over \$1.6 million in grant reimbursements from the Transportation Security Administration's (TSA) Port Security Grant Program (PSGP). The PSGP helps fortify security at our nation's critical ports and maritime facilities. These grant funds are used solely

to enhance security at our sites and to help protect our activities and ports from terrorism, to assist with safeguarding nearby communities and to sustain the flow of commerce in our areas of operations. The Enterprise Security System is being partially funded

"Our Enterprise Security System project is well under way and rapidly nearing completion."

through this program. Non-federal matching funds continue to be applied towards the security project. We are excited about the direction the company is taking to further ensure the security of our employees, customers, and assets.

Security representatives from several Ergon companies such as Ergon Marine & Industrial Supply, Inc., Ergon Refining, Inc., Ergon West Virginia, Inc., Ergon Terminaling, Inc., & Magnolia Marine Transport Company are actively participating in Area Maritime Security (AMS) and local or state security task forces to enhance their security awareness and make possible further vigilance efforts. During a January 2006 AMS meeting held at the United States Army Corps of Engineers District office in Vicksburg, MS, the USCG announced the release of the Department

ATTENTION VISITORS

**ALL VISITORS
MUST CHECK – IN AT
THE OPERATIONS OFFICE**



Dock security is of utmost importance to Ergon.

of Homeland Security USCG Homeport Website at <http://homeport.uscg.mil>. This site serves as a portal to provide information for environmental, health, safety, and security awareness to the public.

Every one of us has the responsibility for doing all we possibly can to safeguard our interests at work and home. Here are a few tips to help you ensure the continued security of your family, friends, and loved ones:

- Develop and rehearse a family security plan that lists steps to take at home or while traveling and provides adequate means of communications.
- Share some basic security “Do’s and Don’ts” with your children.
- Periodically check on the well-being of the elderly.

More of these and other security related tips can be found online at:

<http://www.state.gov/m/ds/rls/rpt/19773.htm>.

Jerry Jerdine
Security Specialist
Ergon, Inc.



<http://homeport.uscg.mil>. This site serves as a portal to provide information for environmental, health, safety, and security awareness to the public.

We Want Your Feedback!

Your opinion counts. One of our priorities is excellent service which balances the needs of all our customers. Please take a moment to share your thoughts and comments about the EHS Department and this publication by using one of the following methods:

- Email us at: ehs.feedback@ergon.com.
- Submit your comments anonymously using the [EHS Survey](#) link on the Environmental page of the Ergon, Inc., Intranet.

ERGON 
a company that works™

P.O. Box 1639
Jackson, MS 39215-1639