

COOP CONNECTION

EMI SIG Continuity of Operations Subcommittee Newsletter



Leadership, Staff, Facilities, and Communications

Using Government Emergency Telecommunications Services (GETS)



By Shonda Barton
Telecommunications Specialist
ActioNet, Inc.

Government Emergency

Telecommunications Services (GETS) is an emergency card service for use on a landline in an emergency or crisis situation when telephone networks are congested. It can also be used in conjunction with Wireless Priority Service (WPS) for added priority service when using cellular networks. During times of emergency, natural disaster, and continuity of operations events, the Department of Homeland Security (DHS) Office of Emergency Communications suggests GETS/WPS subscribers and first responders use their service to ensure priority connectivity to complete a call.

GETS is accessed through a universal number that is provided to authorize priority access to networks for GETS card subscribers when using common telephone equipment. Dialing instructions for using GETS and WPS can be found on the back of the subscriber's card. A series of prompts directs the user to enter a 12-digit GETS pin and the destination phone number. Once authenticated, the call receives priority treatment on the landline network. The user may hear periods of silence when dialing, which is normal, particularly if calls are queued during a heavy congestion. Calls may take more than a minute to complete.

INSIDE THIS ISSUE

Using GETS	1
The Thin Cyber Line	2
COOP Mentors	2
DOE Order 150.1 Rewrite	3
What's New in COOP	3
USFA Guide for Active Shooter Response Released	4
COOP Subcommittee Conference Calls	4
Want to Contribute to COOP Connection?	4

GETS is primarily intended for use when calling within the United States and its territories. Calling privileges can be requested for calls to or from international destinations; however, GETS provides priority treatment only in the domestic segment of the call. GETS calls cannot be made to toll-free (800, 888, 877, 866, 855) destination numbers.

GETS calls can be placed on any cell phone; however, without WPS, priority treatment will not be received until the call reaches a landline network. GETS calls over cellular networks are most effective when used in conjunction with WPS. This is an authorized priority treatment feature on wireless devices. To receive priority treatment on wireless networks, you must register for the Wireless Priority Service (WPS).

There are approximately 127,768 Federal subscribers currently participating in the DHS GETS program. The U.S. Department of Energy presently has 2,208 GETS subscribers.

For further information about GETS and WPS, contact Shonda Barton by email Shonda.Barton@hq.doe.gov or telephone at (301) 903-8660.



The Thin Cyber Line



Dale Hugo Leschnitzer, PhD
Contingency Planning Coordinator
Los Alamos National Laboratory

In August 2012, the Saudi Aramco Company was [hit with a massive cyber-attack](#), which wiped computers' hard drives clean throughout the enterprise. All data and key files were replaced with an image of a burning American flag. In all, over 30,000 machines were rendered inoperable. On machines that were not backed up, all data was lost without any means to recover. It was a true smoking crater scenario.

The good news is that the Saudi Aramco attack hit mainly office computers and failed to accomplish its aim of [stopping oil and gas production in Saudi Arabia](#). It is unknown how many servers were affected. So far, the company is not mentioning if the attack [targeted actual control and oil processing equipment](#).

A Saudi Aramco-style attack would almost certainly create a loss of production and total chaos in an organization. Because of our dependencies on computers and networks, this type of an attack would practically guarantee a continuity event. Many DOE sites have critical computing air-gapped on classified networks. But an attack of this magnitude, even on an unclassified network, would have devastating impacts on personnel's ability to communicate and function.

Los Alamos National Laboratory is holding an internal Contingency Planning Table Top Exercise

based on the Saudi Aramco scenario. While the focus of the Wiper Exercise is truly recovery, there is no doubt that COOP plays a main role in the prioritization of tasks.

It is hard to fathom any private or government organization that has an adequate IT Contingency Plan or COOP Plan that would cover the gamut of problems resulting from a Saudi Aramco-type attack. However, there are many smaller plans that could possibly be tapped. The challenge is that these plans are often maintained by stove-piped organizations that rarely correspond with one another. Just in the IT realm for larger organizations, it is usual for the "desktop" techies and the "network" techies to fly flags of different colors.

What can we, as COOP coordinators, do? Probably the best thing is to start involving these parties together for different functions. Get to know your friendly techies. Invite both IT Management and the IT "boots on the ground" to your COOP exercises. Try to create scenarios where IT is clearly an element. Be careful; do not make them the fall guys! If IT has exercises, see if you can get invited to observe. Talk to your IT Security personnel and discuss the Saudi Aramco attack. Ask their opinions on how your organization prevents such an attack and how they would recover.

Although there is a lot of talk about cyber attacks against critical infrastructure flying around, much of it is hype. The Saudi Aramco attack affected mainly desktop machines. Knowing what attacks are occurring, and more importantly, how they occur and their true impacts, can make you better informed while planning your own site's COOP program.

COOP Mentors

Congratulations to **Thomas Long** of the Strategic Petroleum Reserve for achieving Level I Professional Continuity Practitioner certification.

If you want to join this mentor and receive certification as a Professional Continuity Practitioner, check out FEMA's Emergency Management Institute [Continuity Excellence Series](#). To sign up or to view a complete listing of courses, visit FEMA's [EMI Courses & Schedules](#) site.

U.S. Department of Energy Order 150.1 Rewrite



By Al Cerrone
Continuity Program Manager
U.S. DOE/NNSA NA-41

The Continuity Program Office (CPO) has been comparing notes on federal policy and gathering

input from potential stakeholders concerning the rewrite of the Department of Energy's (DOE) continuity directive, known as DOE O 150.1. The updated Order, DOE O 150.1A, presents a more refined set of standards that creates a more balanced relationship between the President's requirements and those processes that are already infused here in the Department. This update was necessary to stay in line with changing threats and challenges the Executive Branch was facing daily.

The process from the 2008 version to the current Order has not been without its challenges. Offering a practical document that is effective and also meaningful to such a diverse organization as DOE is a daunting task. It began with the 2012 update of Federal Continuity Directive (FCD)-1, which is the implementation document for the National Continuity Policy, and FCD-2. The changes to the FCD brought about, but certainly are not limited to, a renewed emphasis on essential functions, coordinated risk assessments, strengthening the applicability to all levels of the organization, and the incorporation of resiliency into the daily operations of the Department.

These changes necessitated a modification to the governing continuity policy within the Department. Since late February, the CPO has been examining the configuration of the Department and modifying the expectations of both federal employees and contractors to best integrate the President's vision into our reality. We believe we have successfully negotiated a proper balance, while minimizing the potential for interruptions within individual offices and the field. On our current schedule, we anticipate a completed and signed Order in January 2014. In addition to the Order updates, we have almost completed the process of reviewing the Department's Mission Essential Functions (MEFs) (including Primary Mission Essential Functions (PMEFs)) and identifying new/revised essential

functions (PMEFs, MEFs, and Essential Supporting Activities), per the new requirements of FCD-1 and the instructions laid out in FCD-2. Our current schedule is to have the revised MEFs and PMEFS ready for senior leadership approval in June 2014. The DOE COOP Plan will be updated soon after to incorporate the required changes in the Order and to reflect the refined MEFs. If there are any questions, please contact the CPO at (301) 903-3766.

What's New in COOP

FEMA has updated its Continuity Assistance Tool and two continuity planning documents, now available [here](#). These documents are provided for state, territorial, tribal, and local governments to assist in their continuity of operations planning, which ensures that essential functions and services can be continued during, or resumed rapidly after, emergencies. Included are these updated documents:

- **Continuity Assistance Tool (CAT)**
- **Continuity Guidance Circular 1**
- **Continuity Guidance Circular 2**

FEMA's Citizen Corps Whole Community and CERT Core Capabilities Tool Now Available

FEMA's Individual and Community Preparedness Division has completed and released the Citizen Corps Whole Community and Community Emergency Response Team (CERT) Core Capabilities Tool. This tool can assist State Administrative Agencies (SAAs) in demonstrating how Citizen Corps and CERT programs support most of the target capabilities and help implement the whole community approach to emergency management. This tool can help SAAs and Citizen Corps Councils at all levels develop strategic investment justifications with a high return on investment. Download the tool and related documents [here](#).

USFA Guide for Active Shooter Response Released

The U.S. Fire Administration (USFA) has released its guide to support planning and preparation in advance of an active shooter and mass casualty incidents.

[Fire/EMS Department Operational Considerations and Guide for Active Shooter and Mass Casualty Incidents](#) is one of many resources available for agencies to prepare themselves to respond to an event in their community.

Details within the 17-page report offer assistance in what a Standard Operating Procedure should contain, ideal on-scene interagency practices, managing “reverse triage,” and maximizing survivability in those injured.

It can be complicated to navigate and respond to incidents that involve multiple agencies, states, and levels of government. USFA recommends training and planning with every agency that may become involved in such an incident in order to make an already difficult situation less chaotic.

The Department of Justice has also released its [Active Shooter Event Quick Reference Guide](#), which provides tips for how to respond in an active shooter event.

COOP Subcommittee Conference Calls

COOP Subcommittee conference calls typically occur on the second Thursday of each month from 3-4 p.m., Eastern. The schedule for the next four calls in 2014 is below.

- Thursday, Jan. 9
- Thursday, Feb. 13
- Thursday, March 13
- Thursday, April 10

Agendas are sent prior to each call. If you have questions about the COOP Subcommittee conference calls, please contact Becky Bullard at Becky.Bullard@orau.org or (865) 576-9623.

Want to Contribute to COOP Connection?

If you'd like to contribute continuity stories, calendar items, or any other news related to COOP, please send them to Becky Bullard at Becky.Bullard@orau.org or to Jeff Morrison at morrisjl@nv.doe.gov. The deadline for submissions for the April issue is March 6, 2014.

