PROTECTING PERSONAL AND SENSITIVE INFORMATION

A training course for REACT Teams and members

This is the second of a series of short courses for REACT members to train to perform communications duties in specific disaster response roles.

Author: Walter G. Green III

Course Number: 103B

REACT International, Inc.
P.O. Box 21064, Glendale CA 91221
e-mail: Training@REACTintl.org
(866) 732-2899 / Toll Free (US Only)
(301) 316-2900 / International
(800) 608-9755 / Fax

Table of Contents

I. INTRODUCTION

In a disaster or major emergency information becomes central to an effective response. At the same pressure builds to forward that information to the people who need it as quickly as possible. How you pass it on becomes less important than passing everything you know over whatever means of communication is available.

As normal communications become disrupted that often means in plain text over the radio. With the discovery of Zello by volunteers, that information can often flow over an Internet communications circuit on which anyone can listen. In the heat of the event, everyone can know what is happening, and that is a good thing. Right. Isn't it?

In simple terms, NO. Much of the information that flows in a disaster involves either privacy or operational sensitivity concerns. General access by anyone means that anyone can violate the privacy of those impacted by the disaster. General access by criminals, rioters, looters, etc. means that anyone with bad intent can find the most vulnerable points to carry out their activities. And, in a terrorist incident, general access by the terrorists simplifies assessment of the success of the attack, evasion of law enforcement, and targeting of rescue forces with secondary devices.

The problem of emergency and disaster communications is to ensure the right information makes it to the right users while protecting that information from disclosure to those without a right to access it. That means that we must protect information from disclosure by procedures that establish what we can say over a radio, in an e-mail, etc., and by the selection of transmission means that limit the access of persons not entitled to know that information.

And that is what this course is about …

II. FIRST

A variety of different standards define what information should be protected. Some of these are laws, such as the Health Insurance Portability and Accountability Act which protects patient medical information. Some are the standards or regulations of the organization that originates the data. And some are accepted best practices. You cannot be expected to know or understand all of the different information protection requirements that exist. However, if you violate one of these requirements, you can expect anything ranging from severe disapproval and loss of

confidence by the organization in your Team's ability to perform emergency communications all the way to legal liability. This means that you must:

(1) Understand the basic principles of information protection and be able to identify information that possibly may require protection.

(2) Use operational procedures that provide the most protection possible within the general Federal Communications Commission requirement that you may not disguise the meaning of your transmissions.

(3) If you are the originating station for a message, make sure that the individual providing the message text has considered whether the information in the message needs to be protected.

III. GENERAL PRINCIPLES

Three general principles govern how personal and sensitive information is managed:

(1) Confidentiality – personal and sensitive information must be accessible only to those authorized to see or hear it, not to those who wish to see it just because it exists or because they think they are entitled to see or hear it. There must be a need to know.

(2) Integrity – people without authorization to make changes to the information should not be allowed to make changes.

(3) Availability – people who have permission to see or hear the data must be able to do so.

IV. PERSONAL INFORMATION

Personnel information is any information that allows the identification of a specific person or persons impacted by a disaster.

Disaster response, recovery, and relief organizations have an ethical, and in many cases a legal, duty to protect this information from disclosure. If you do disclose personal information, and it comes to the attention of an organization you are supporting, you can expect that organization to discontinue any relationship with

you and your Team immediately and permanently. They simply cannot afford the legal consequences of your negligent acts.

Examples of core personal information include:

- Name
- Physical address
- E-mail address
- Telephone number
- Social Security Number

However, this is not a complete list of personal information that might require protection. Depending on the situation association of any of the following information with an individual may need protection:

- Identification of the medical condition or medical treatment of an individual – this may also violate health privacy laws.
- The individual is deceased – initial death reports of individuals should never be transmitted over radio or unsecure Internet systems.
- Identification of gender or gender preference.
- Financial information – for example, transmission of credit card numbers over an unsecure means is an obvious invitation to identity thieves.
- Reference to race, ethnicity, or national origin.
- Identification of religious affiliation.
- Age, especially of children and the elderly.
- Recovery file or case numbers

When information stops being personal the level of protection required may be reduced, again depending on the situation. Aggregated information, such as the number of injured and the number of fatalities, is not personal information and does not require protection as such.

As an example, consider the following examples of potentially personal information and the degree of protection needed:

- Hurricane Alfonso has caused 23 deaths in the United States. [no personal information]

- Two of the deaths from Hurricane Alfonso occurred in Georgia. [no personal information]

- One of the deaths from Hurricane Alfonso occurred in Brunswick, Georgia. [no personal information but may be sensitive information – depending on the situation protection may be required]

- The person killed by Hurricane Alfonso in Brunswick, Georgia, lived at 22 Prince Street. [personal information and potentially sensitive information – protection is required]

- Ms. Babette Smith, a 22 year old transgendered female living at 22 Prince Street, Brunswick, Georgia was killed when a tree fell upon her house in Hurricane Alfonso. [personal information and potentially sensitive information – protection is required]

V. SENSITIVE INFORMATION

Sensitive information includes any information that is not specifically personal information and that needs protection from disclosure. This includes information that is (1) operationally sensitive and that is (2) individually sensitive. Some sensitive information will need protection for only a short period of time, but other information may need to be protected permanently. For example:

- Protection for a relatively short period of time - the names of individual killed in a disaster is sensitive information until the list of names is released by the medical examiner or coroner.

- Protection permanently – your Team's procedures for dealing with harassment or intrusion into communications during a disaster response is something that needs to be restricted to Team members permanently.

OPERATIONALLY SENSITIVE INFORMATION

Operationally sensitive information is information that, if revealed, can impact the outcome of an emergency response. This includes information that:

(1) Could compromise the safety of individuals and units responding to the emergency. This ranges from revealing key locations such as staging areas or the

location of the incident command post to personal details such as key leadership assignments in the response. In the short term it may include routes of travel, timing of operations, numbers and types of units involved, etc. Longer term protection may be required for emergency operations plans and emergency procedures.

(2) Could allow harassment of the responding organizations during the emergency response. This includes the problem of pranksters, hackers, and others for whom intruding into communications and insertion of false information or just streams of obscene language is either a fun activity or serves political or other purposes.

(3) Needs to be protected until it can be released by an appropriate authority. This category includes information that has not been verified, information that has to be released only after notifications have been completed (for example, notifications of next of kin), and information that requires a decision as how it will be released.

INDIVIDUALLY SENSITIVE INFORMATION

Individually sensitive information is information that may not meet the standard of personal information in the law, but that, if revealed, may cause some harm or distress to the individual. A good, informal test is to ask yourself "would I want this to be broadcast to my community over a Citizens Band or Amateur Radio so that everyone will know it about me?" This includes:

(1) Unconfirmed identifications – a good example of this is the discovery of human remains that you can assume may be those of a missing person. Until the remains are identified the possibility that they may be the individual is sensitive.

(2) Death notifications – until the next of kin have been notified, announcements of death are a borderline personal information, operationally sensitive information, and individually sensitive information.

(3) Criticism of the victim – the classic individual criticism that you do not want to transmit is what a public information officer once said, "the individual died because he was stupid." The classic group criticism that you do not want to transmit is what a national political leader said in a recent hurricane disaster, to the effect of "that the victims needed to step up and do more for themselves." Not only are these heartless, but ill-considered remarks can do far more damage to you than to the person you criticize.

VI. WHAT METHODS ARE MOST VULNERABLE?

Every possible method of transmitting information from one point to another is vulnerable to that information being compromised. The question is how vulnerable. Highly secure systems are just that, but they rely on procedures, cryptological materials, encryption devices, and hardened physical security that we as volunteers will never need or have access to. However, it is important to understand the degree of vulnerability of the systems we do use. The following table provides a look at the relative vulnerability of different approaches to having the data exposed and misused.

Vulnerability Level	Type	Vulnerable To	Use For
Very High	Unsecured Internet forums, chats, social media, and bulletin boards	Anyone can listen to and copy information from these sources	Do not use
Very High	Unsecured Zello	Anyone can listen to information on this source	Do not use
High	Any personal radio service	Anyone with a radio in the same service	Use for uses that do not include sensitive or personal information
High	Amateur Radio voice nets	Anyone with a radio in the same service	Use for uses that do not include sensitive or personal information
Moderate +	Amateur Radio Winlink and Echolink	Requires an amateur radio license, technical sophistication, and appropriate equipment	Use for uses that do not include sensitive or personal information
Moderate	Password protected bulletin board or Zello	Failure to randomly change passwords greatly increases vulnerability	Use with caution

Low +	Fax and e-mail	Accidental use of incorrect addresses, hacking, unattended fax machines	Use with attended fax machines and strong security software
Low	Amateur Radio data transmission	Amateur radio operator with compatible equipment and software and knowledge of operating procedures	Unrestricted use

VII. STEPS FOR PROTECTION

The first and most important defense - do not transmit information that reasonably requires protection unless you have permission in writing from the individual whose information it is or from the appropriate agency that has originated the message. If there is any doubt advise the originator that you have concerns that the information may be personal or sensitive and request confirmation of its appropriateness for transmission. Make certain that you record the name and title of the individual giving permission as a notation on your copy of the message, along with the time and date. Failing to adhere to this standard may result in a very unfortunate outcome for you and/or your Team.

Second, carefully consider the time sensitivity of information, the information's relative importance, and the threat level in deciding what to transmit and what method of transmission to use. Some sensitive information may be of high importance and require immediate transmission, justifying its transmission on voice circuits even with elevated risk. If you are in doubt about how information should be handled during any event, ask the agency you are supporting for guidance on what they consider sensitive information and how they want it protected.

Third, look at your procedures carefully. If you always use on frequency or channel for one purpose, it may be time to change to another. If you support a public event at the same location in the same way, find a different way to perform your support next year. Although terrorism and mass shooting events will generally not involve a REACT Team response, events like the recent Las Vegas mass shooting show careful scouting by the perpetrators and observation of prior events.

Fourth, have a plan to protect your frequencies from interference. Do not acknowledge deliberate interference; doing so tells the responsible person that they are being effective. Harassing transmissions or deliberate jamming can be defeated, at least temporarily, by having a preplanned series of shifts from one channel or frequency to another keyed by transmission of a code word (the code word should not identify the interference as the reason).

Fifth, do not ragchew on the radio when you are bored. You are involved in the event to provide a service, not to chat with your radio buddies. You may inadvertently disclose sensitive information without thinking just to keep the conversation going or to impress other people on the frequency or channel. Do not discuss event details with stations that are not part of the event. If you encounter persistent interest or questions from a station that you do not know, immediately report the fact to whoever is in charge of event security.

Sixth, practice good paperwork control. Do not leave plans, procedures, or messages unsecured in places where someone could pick them up. Have an organized system for filing messages during the event, with a container that protects them from loss (as simple as a small portable file box). Do not discard papers with sensitive or personal information in the trash – shred them. Small portable shredders are available in any office supply store, and are an essential part of any emergency radio station.

Seventh, practice good equipment security. Do not leave your station unattended in a location where people not associated with the response or event can access it.

Eighth, practice good operational and personal security. Do not discuss how, when, and where in social media or in Internet forums. Americans are amazingly free with details of their lives and interests – that information is valuable to criminals and terrorists. For example, more than one family has been rewarded for discussing their travel plans on social media by having their house burgled while they were away.

The discussion above may sound overly alarmist. Understand that your supported agencies are concerned about protecting personal and sensitive information. There are people who will exploit disaster victims at the first opportunity given their identity and address, there are criminals who will exploit unattended property if you tell them where it is, and there are terrorists who will exploit weaknesses in response. All of these have happened in the last decade in the United States. Don't let it happen on your watch because you were careless.