

## Keeping Your Security Measures Secure

**E**nhancement of security measures by water and wastewater utilities is a given in today's environment. Moreover, such measures have become more than a matter of sound management. The requirement for preparing and filing vulnerability assessments and response plans under the new federal Bioterrorism Act make such steps essentially mandatory.

One issue that can be overlooked inadvertently is how to maintain security over the security measures taken. In other words, what steps can a utility take to protect its security plans from disclosure?

### Who Needs To Know?

Within a utility organization, it is doubtful that security plans need to be, or should be, widely disseminated. Such plans should be limited to as small a universe as possible—basically the personnel administering the security, and to the extent of their involvement.

Of course, some measures always will be publicly obvious: for example, a chain link fence, with razor wire and a padlock. However, other measures are not obvious: for example, remote sensors and how they are monitored. There is no need to disclose such measures to persons who have no need to know them.

In the case of personnel given security knowledge, background and credentials should be verified and non-disclosure agreements should be executed. In the case of outside consultants such as engineers, attorneys, accountants and vendor representatives, additional steps may be justified.

### Disclosure at Meetings

Control over disclosure of security details may be easier within the confines of investor-owned utilities. However, municipal-owned utilities may have to deal with open-meeting laws as may be applicable to municipal city councils and village or district boards.

Most public meeting laws have provisions that permit closed or executive sessions under stated circumstances and may provide that the minutes of such sessions are protected from disclosure. Obviously, if the specifics of security measures must be discussed, every effort should be made to do so properly within a closed session. In those jurisdictions where this is not possible, it may be necessary to request the legislature to modify the laws.

### Freedom of Information Requests

Municipalities are subject to the Freedom of Information Act (FOIA) laws of their respective states. If sensitive security information were required to be disclosed under a FOIA request, the security measures implemented likely would be compromised.

Simply stated, it makes no sense to have to disclose security plans under a FOIA request.

The federal Bioterrorism Act exempts vulnerability assessments filed with U.S. EPA from FOIA disclosure. Some state laws also would exclude security disclosure under a FOIA request. Some states, including Iowa and Virginia, recently have enacted such exceptions to their FOIA laws.

If the FOIA laws in a particular state do not have an exception that would encompass sensitive security information, then efforts should be made promptly to change such laws.

### Regulatory Disclosures

Regulated water and wastewater systems generally are subject to administrative agency disclosure requirements. For example, in a proceeding for approval of a rate increase, a regulatory agency may wish to audit the amount or reasonableness of costs incurred or projected for security measures.

Even at this level, sensitive security information should be protected from unnecessary disclosure. One way to accomplish this is to make such information available to agency staff only at the utility's premises and under its supervision; to require that the agency certify a particular staff person; to require a non-disclosure protective agreement by that person; to bar reproduction of any documents; and to code documents so that they can be accounted for before the staff person leaves the premises. It also may be advisable to have the agency issue a protective order, particularly if intervening parties are involved. In the case of court litigation, comparable steps should be taken. See the *Resolution on Commission Procedures Related to the Increased Security Measures Undertaken by Water Utilities*, adopted by the National Association of Regulatory Utility Commissioners, November 13, 2001.

### Other Security Measures

Obviously, there are some administrative measures that utilities can take to minimize disclosure of sensitive material. Websites can be filtered to delete security information. Computer access to data can be restricted. Plans, specifications, manuals and contracts should be secured. Shredders can be used when documents no longer are needed. Public reports, including utility annual reports, statements under GASB 34 and consumer confidence reports should exclude specifics about security measures.

*For a review of state FOIA laws and models for protection of security information, see State FOIA Laws: A Guide To Protecting Sensitive Water Security Information, published by the Association of Metropolitan Water Agencies.*

