Pipeline

Small Community Wastewater Issues Explained to the Public

Preparing for the Unexpected: An Assessment Process for Small Wastewater Systems

Your wastewater treatment system is an important part of the community as it protects both public health and the health of the environment. As a foundation for your local economy, it represents a sizable investment, and so it needs to be adequately protected in time of emergency.

Natural disasters, operator errors, terrorism, vandalism, and even curious children, are potential hazards for a small wastewater treatment system. Is your system located in a floodplain? Is it in an isolated area and often unstaffed? Is your collection system spread over a large area and easily accessible to unauthorized people? Are there specific countermeasures you can put in place now to reduce the vulnerability of certain areas?

These safety and liability concerns are always present, but in this time of renewed caution due to the recent national events, it is a good time for local decisionmakers and system personnel to perform an assessment and to review their emergency operations plans.

No community will ever be able to anticipate every problem or event that might occur, nor will every emergency be avoided. But by conducting an assessment, you can determine the most likely threats and those that would have the greatest impact on the system and prepare accordingly.

This assessment process involves:
1) recognizing your system's assets,
2) identifying potential threats,
3) defining the systems' vulnerability to these threats, and 4) developing plans of action in response to the emergency. The end result of this process is an improved ability to prioritize and implement effective actions, safeguarding your community's public health, economic assets, and environment.

This issue of *Pipeline* is intended to serve as a guide for decision makers when considering the vulnerability of their wastewater treatment system as described in *Protecting Your Community's Assets: A Guide for Small Wastewater Systems* recently published by the National Environmental Training Center for Small Communities. Details about how to obtain a copy of this new publication are on page 7.
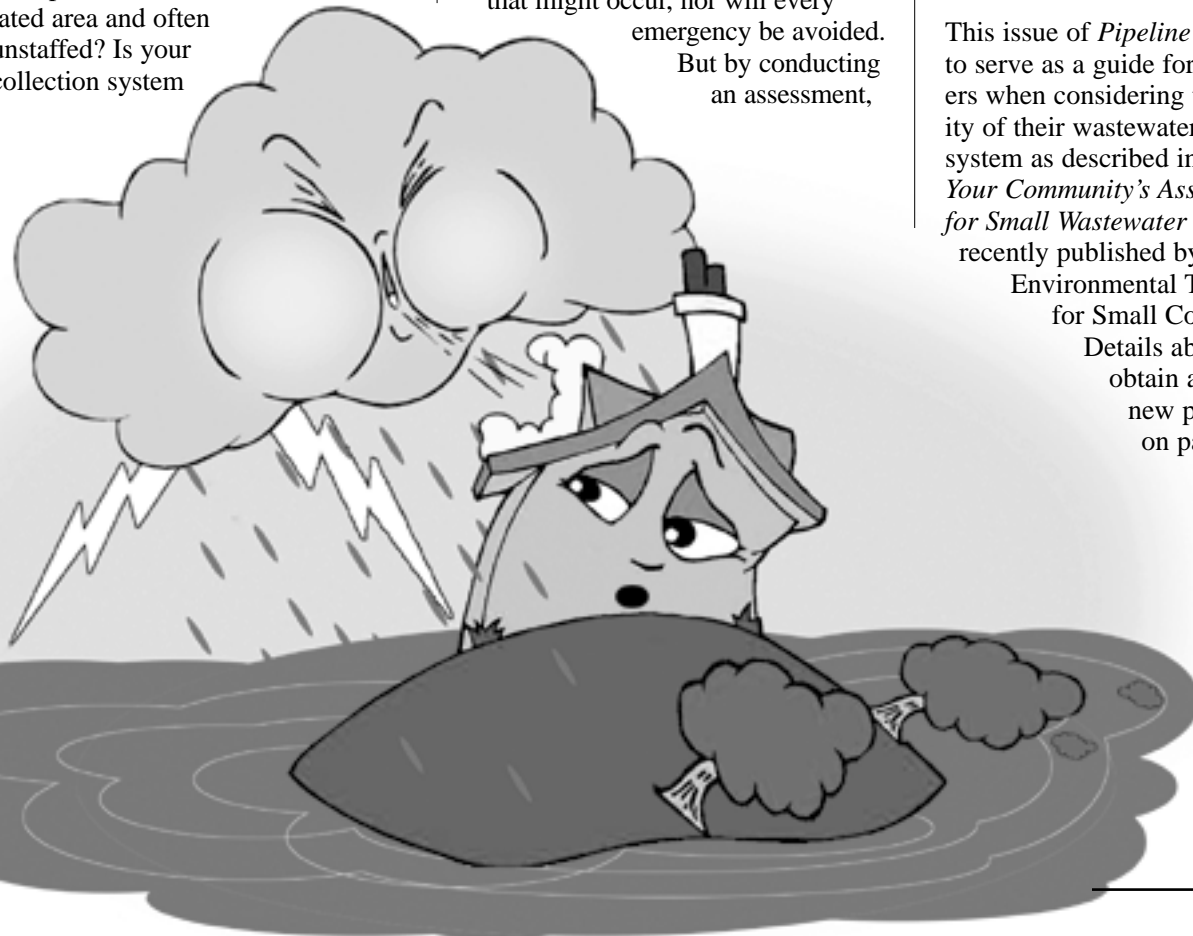
Identify your system and your assets

Start by determining the major assets of the system. Most small systems will only need to consider the physical infrastructure and the human component consisting of employees and customers. Larger systems might have computer systems that are vital to the operation and/or contain customer records that need to be safeguarded. It is important to carefully list all of your assets.

The employee category must include everyone on the payroll — part-time plant workers to office staff. Customers may include residential and industrial customers plus contracts you may have with commercial septage haulers.

Besides the buildings, the physical plant includes the treatment areas (preliminary, primary, and/or secondary), residuals handling and disposal, disinfection processes, chemical storage, and laboratory facilities. The collection system is also a facet of your operation and is vulnerable to disruption. Consider the number, type and location of manholes, cleanouts, sewer pipes, and lift stations as part of the physical component. It may be helpful to list all your assets with a brief description and any special information that might be important.

Identify threats

After reviewing and listing the vulnerable areas of your system, it is important to list and consider all potential threats and to determine how likely they are to occur. See the table on this page for a listing of possible events that could lead to disaster for your system. Some of these threats may have already impacted your system. Others will be completely unlikely for your geographic area, and may be disregarded. But wise managers will consider all possible threats, even ones from terrorism or other intentional acts. If the point of terrorism is to create public fear and disrupt normal society, wastewater treatment plants are perfect targets. They are relatively unguarded, house hazardous chemicals, and the interruption of their service leads to threats to public health.

If the point of terrorism is to create public fear and disrupt normal society, wastewater treatment plants are perfect targets. They are relatively unguarded, house hazardous chemicals, and the interruption of their service leads to threats to public health.

A list of natural disasters that may effect your plant's operation could include: hurricanes or high winds, winter storms and blizzards, floods or drought, landslides or mudslides, thunderstorms and lightning, forest or brushfires, and floods. Earthquakes, avalanches, and volcanic eruptions are extreme possibilities.

Other disruptions might include sewer blockage, a construction or transportation accident, and energy disruptions such as a gas line or water line break. Explosions, arson, strikes or riots, and criminal vandalism must also be considered as potential threats to your operation. Harmful inputs to the system that would halt or reduce your effective operation might be the release of hazardous, high-strength organic, chemical, or radioactive materials.

When considering all possible threats to the operation, disruptions in communication systems can be crippling. Think how dependent your operation is on telephones and two-way radios.

For treatment plants with extensive computerized operations, the threat

Threat List

Natural disasters
Flood
   River
   Stream
   Low-lying areas
   Dam break
   Snowmelt
Landslide
Thunderstorms and lightning
Tornado
Hurricane
High winds
Winter storms and blizzards
Freezing
Drought
Extreme heat
Forest or brushfires
Earthquake
Avalanche
Volcanic eruptions

Manmade disasters (intentional and unintentional)
Equipment failure
Human error
Fire
Construction accident
Transportation accident
Explosives
Guns or other weapons
Energy disruptions
Gas line break
System blockage
Lift station failure
Release of sludge/effluent
Arson
Trespassers
Vandals
Criminal acts
Strikes
Riots
Terrorist attack

of Supervisory Control and Data Acquisition (SCADA) system failure or system invasion by hackers is a possibility.

Threats to your system are varied, and you must consider all possibilities or combinations and take corrective actions for each potential threat.

Assessing vulnerability

Records
Records, maps and other information should be stored in a secure location. Make backup copies on a regular basis and store them off site. A complete copy of your system's emergency response plan (ERP) should be safely stored off site also. (Find more discussion about ERPs on page 6.)

Computer system protection
Computers and computerized controls like a SCADA system are becoming much more common in small wastewater systems, and can be vulnerable to all sorts of problems.

You should use passwords and change them frequently. If possible, each employee should have a unique password not shared with others. Install virus protection software and upgrade it regularly Install a firewall protection program to prevent outside

access. If you use a modem, install software that will disable the local network connection when the modem is not in use. Make backup copies of computer data routinely and store them at a secure off-site location. Web sites should not contain critical information about your system. If you use a SCADA system, it should be tested for vulnerability.

To prevent damage to your computer equipment during a flood situation, do not locate it in the basement or other low area of your facility. It is also wise not to store any electronic equipment on the floor. Surge protection equipment will reduce damage to your electronics from lightning strikes.

Perimeter and access control
Restrict access to the physical plant. To secure the main treatment plant and outlying components, such as pump stations, consider issuing photo identification cards for employees and posting signs restricting entry to authorized personnel only. Ideally, all facilities should be enclosed with a security fence with locked gates. Keep fence lines clear of vegetation and remove objects that could be used to gain entry, such as large rocks, cement blocks, or ladders. Adequate lighting and frequent patrolling by the staff may discourage potential tampering. Watchful neighbors can be very helpful to a security program. Install an alarm system that notifies the proper authorities if there has been a security breach. Consult with your local law enforcement agency about selecting an alarm system.

Hazardous material control
Maintain material safety data sheets (MSDS) for all chemicals used, and all employees should be trained in reading them.

Store chemicals appropriately in a secure area. It's important to keep equipment at hand to facilitate a rapid response to an emergency.

Provide the local fire department information about the hazardous materials stored and used at your plant, and do not respond to a release for which you are not properly trained or equipped. Instead, coordinate training with local emergency response personnel well before an emergency occurs.

Protecting the process
There are several low-tech and low-cost things a plant operator can do to help keep things running even in the event of an emergency.

Abnormal influent or effluent odor and color can be simple hints of trouble. Establish a baseline that will allow you to check for any change that indicates possible contamination. Make sure that all personnel are familiar with the controls of critical components, in the event that regular operators are unavailable. Keep fire extinguishers and other emergency equipment in good working order, and make sure that all employees know how to operate them.

nesc **3**

The routine maintenance of critical parts of your process is essential. Routinely inspect lift stations, generators, emergency pumps, valves, etc. And since disruption of services to critical customers can cause serious problems, secure all points of the collection system.

Human assets

Your personnel and customers are vital assets; therefore, it is essential to protect them and their interests.

Personnel have easy access to the plant and so should be hired only after obtaining the utmost confidence in their work ethic and background. Good hiring practices include completed applications and verified references. Background checks may prevent potential security issues. Require terminated employees to turn in keys, access codes, and other security related items.

Train employees about security issues, including what to look for and how to report any suspicious activity. All personnel should know whom to contact in the event of an emergency. Training is essential for a well-prepared operations and support staff. Training needs to be appropriate for each individual's responsibilities. If possible, routinely conduct emergency training exercises with the appropriate local emergency responders.

Your emergency plan should address public health and medical issues. Specifically consider procedures to identify and treat victims, evacuation procedures, or instructions for in-place sheltering. The emergency plan should also consider the personal safety of emergency responders.

Educate your customers about their wastewater system. Regularly send out information with bills to explain
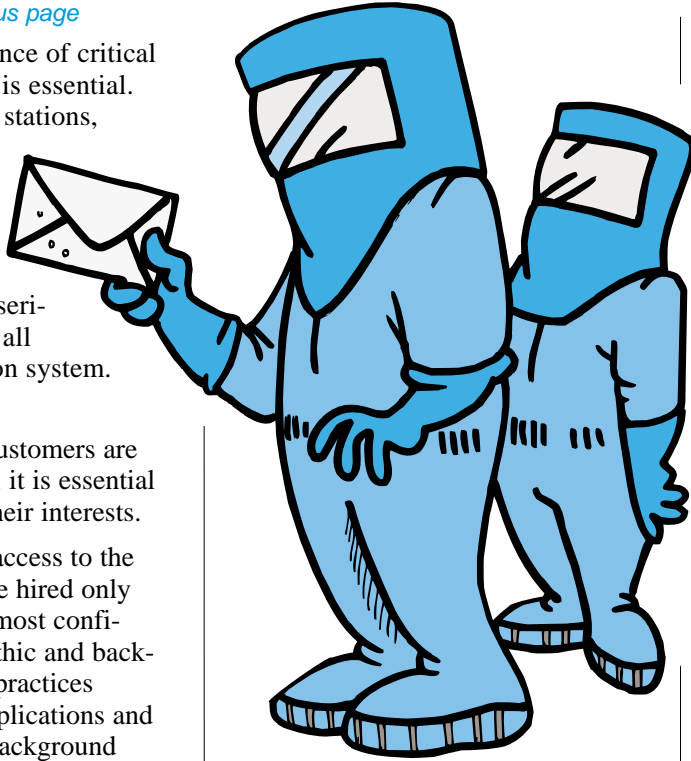
ways users can help protect the community's investment. It is beneficial to have a procedure in place to advise customers about the health risks a disruption of the wastewater system can cause. In the event of a security breach that results in a potential health hazard, you must notify the public via all media outlets; i.e., radio, television, door-to-door, and posting in public places. Advise customers about potential hazards, and give them information on proper precautions.

Prioritizing corrective actions

After completing the asset analysis and vulnerability assessment, decision makers should identify any possible corrective actions. Rank these countermeasures according to how effective they are based on the extent to which they will reduce the risk of significant and negative public health impacts. Consider both economic and social impacts. Further determine whether the corrective action is feasible for your

community. For major changes and improvements, potential funding help is detailed on page 6. Yet there are many low-tech and low-cost measures.

Some low- or no-cost suggestions are:

- Keep access roads to major system assets clear and passable.
- Install a backup power source.
- Provide identification for all employees.
- Keep all locks locked and gates closed and secured.
- Protect lab and computer equipment with power surge protection.
- Back up computers regularly.
- Keep safety equipment (personal protective equipment) on hand for all employees.
- Post "No Trespassing" or "Authorized Personnel Only" signs at key points.
- Raise all supplies and equipment off the floor.
- Store copies of all paperwork in a remote location.

Emergency response plan

An ERP is a document that spells out in detail your system's plan of action for responding to emergencies, disasters, and other unforeseen events. It may also be known as an emergency operation plan or emergency management plan. By doing all the necessary paperwork and making the appropriate arrangements before an emergency, you'll have everything at your fingertips should an event occur.

It is essential to prepare an up-to-date ERP specifically prepared for your facility. Contact your state emergency response commission or local emergency planning committee for help. Many local and county governments already have emergency response plans in place. Find out about existing plans in your area and how your treatment system ties into the plan. Only share the ERP with local first responders (police, fire,

Top Ten Most Common Errors Found with Emergency Response Plans

1. No upper management support
2. Lack of employee buy in
3. Poor or no planning
4. Lack of training and practice
5. No designated leader
6. Failure to keep the plan up-to-date
7. No method of communication to alert employees
8. Occupational Safety and Health Administration regulations are not part of plan
9. No procedures for shutting down critical equipment
10. Employees are not told what actions to take in an emergency
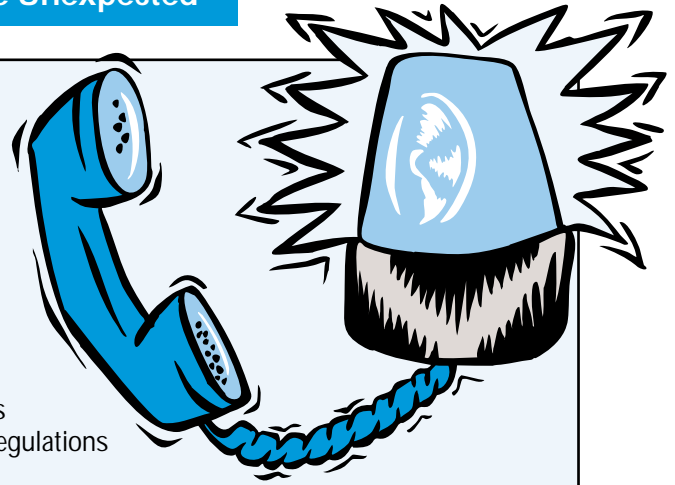
Source: National Safety Council

and emergency medical), and do not post it for public viewing since it gives people information that could be used against the system.

Wise managers determine how vulnerable your system is to various calamities that might render it inoperable and decide the most appropriate response to potential emergencies before they occur. The key to being prepared is to identify conditions that are likely to happen during an emergency, and then to minimize the vulnerability of critical assets that are likely to be affected. Your goal as a prepared manager is to reduce risk—first reduce the risk to people, then to the process, then to the physical plant. Basically an emergency response plan determines who will do what, when, with what resources, and under what authority.

The first step in developing your ERP is to develop an Emergency Contact List. (See example at right.) Someone must be available to respond to an emergency regardless of day or time. This contact information must be kept up-to-date and made available to all system personnel, local officials, and local first responders. (It is wise to get to know your local first responders before an emergency develops.) If you suspect terrorism, you must contact special agencies. See the side bar on page 6 for details about addressing terrorist activities.

To make your emergency plan as complete as possible, get input from all groups and individuals who have decision-making and operational responsibilities for your wastewater system. This may include plant workers as well as such agents as members of the town government, legal advisors, and local emergency personnel. Involve human service organizations such as the Red Cross, also. These organizations provide crisis counseling, insurance information and assistance, and translation services during time of emergency. This wide range of input will address the broadest scope of possible events and produce the most effective emergency plan.

An ongoing process

Remember that emergency preparation and installing security measures at your facility are ongoing processes. Review and update your preventive and response plans annually. Preparedness is not an end point, but a goal that can be achieved only through continued efforts to assess and improve the overall security of your system.

Emergency Contact List

NPDES# _____

System Name _____

Town/City _____

Telephone Numbers
System Telephone_____

Evening/Weekend Telephone_____

Other Contact Information
System Fax _____

Email_____

Population Served and Number of Service Connections
People Served _____

Connections _____

System contact
Name and Title _____

Telephone _____

nesc **5**

Funding for Security Measures

You may be able to finance some of the expenditures required to adequately protect your publicly-owned treatment works (POTW) through the Clean Water State Revolving Fund (CWSRF).

States may use CWSRF monies to provide low or zero percent interest rate loans to municipalities for wastewater infrastructure as well as to ensure protection from security threats and vandalism. States may provide CWSRF assistance to communities to allow them to complete vulnerability assessments and contingency and emergency response plans.

Many of the types of infrastructure improvements a system needs to take to ensure security may have already been included within the scope of infrastructure projects funded

through the program to date. The table below identifies some specific security activities the local decision makers might consider and whether or not the activity is eligible for funding through the revolving fund program.

If a community is interested in obtaining financing to implement security measures, the first step is to contact their state's CWSRF representative through the EPA's Office of Wastewater management Web site at *www.epa.gov/owm/finan.htm.*

Source: EPA, Office of Water, "Use of the Clean Water State Revolving Fund (CWSRF) to Implement Security Measures at Publicly-owned Wastewater Treatment Works," EPA 832-F-01-008, November 2001.

If you suspect terrorism…

The U.S. Environmental Protection Agency (EPA) is currently working with the water industry to provide information about security precautions and technical assistance to states and utilities. The EPA is working in collaboration with the Association of Metropolitan Water Agencies and other groups to develop an information sharing and analysis center to provide coordinated notification and response to threats. For additional information, you can visit the following Web sites:

EPA Counter-Terrorism: *www.epa.gov/ebt-pages/ecounterterrorism.html*

EPA Alert on Chemical Accident Prevention and Site Security: *www.epa.gov/ceppo/ppubs.secale.pdf*

U.S. Centers for Disease Control & Prevention: *www.bt.cdc.gov*

Association of Metropolitan Sewerage Agencies: *www.amso-cleanwater.org*

Association of State and interstate Water Pollution Control Administrators: *www.asiwpca.org*

National Governors Association, Emergency Management and Terrorism: *www.nga.org/center/topics*

National League of Cities: *www.nlc.org/nlc_org/site/newsroom/terrorism_response*

Eligibility for funding of various security measures

Type of Activity	Eligible under CWSRF
General	
Vulnerability Assessments	Yes
Contingency/Emergency Response Plans	Yes
Facility	
Security guards	No
Fencing	Yes
Security cameras/lighting	Yes
Motion detectors	Yes
Redundancy of systems and power	Yes
Secure chemical and fuel storage	Yes
Lab equipment	Yes
Monitoring	No
Sewer System	
Securing large sanitary sewers	Yes
Tamper-proof manholes	Yes

Reprint Info

Readers are encouraged to reprint *Pipeline* articles in local newspapers or include them in flyers, newsletters, or educational presentations. Please include the name and phone of the National Small Flows Clearinghouse (NSFC) on the reprinted information and send us a copy for our files. If you have any questions about reprinting articles or about any of the topics discussed in this newsletter, please contact the NSFC at (800) 624-8301.

Workbook and Software Package Offer Additional Help

The National Environmental Training Center for Small Communities has developed a workbook-style guide specifically designed to assist small communities in identifying vulnerable components of their wastewater system and prioritizing appropriate corrective actions. It is available free to download from the Website *http//:www.netc.wvu.edu*. Titled *Protecting Your Community's Assets: A Guide for Small Wastewater Systems*, it takes local decision makers and system personnel through the process described in this issue of *Pipeline*. Easy-to-use checklists are provided for taking inventory of assets, assessing threats and assessing vulnerability. A systematic framework is outlined that ranks potential corrective actions and establishes appropriate priorities for needed actions.

Larger communities and smaller systems with computer capabilities and a desire to use more sophisticated ranking approaches may want to consider using the electronic Vulnerability Self Assessment Tool (VSAT) provided by the Association of Metropolitan Sewerage Agencies. This software package is available free for downloading from their Web site: *http://www.vsatusers.net*.

National Safety Council Booklet Provides Step-by-Step Action Plans

The On-Site Emergency Response Planning Guide is available from the National Safety Council (NSC) to introduce the strategies and methods behind emergency planning for both manmade and natural disasters. The guide provides specific action plans to cope with hazardous material emergencies, structural failures, evacuations, bomb threats, medical emergencies, armed robbery, earthquakes, and tornadoes. It also provides templates on its companion computer disk (included with the booklet) that help the user create and implement an emergency response plan.

These emergency response procedures comply with

Occupational Safety and Health Administration (OSHA) standards and are used at NSC headquarters. The guide offers a toll-free number and e-mail address so readers can get technical support when using the recommended procedures. For more information about the *On-Site Emergency Response Planning Guide* (product #12212-0000) or to order, visit the NSC website or contact them at (800) 621-7619.

The NSC is a not-for-profit, non-governmental, international public service organization dedicated to protecting life and promoting health. For additional information about the NSC and its emergency planning programs, visit their Web site at *www.nsc.org*.

Homeland Security: Resources for Local Governments

Practical Tools for Local Governments

The National League of Cities is making available several useful publications through their Web site, *www.nlc.org* or by phone at (202) 626-3000. New guidebooks are available with key issues focusing on specific aspects of assessing threats and being prepared.

The National League of Cities is the oldest and largest national organization representing municipal governments throughout the United States. Its mission is to strengthen and promote cities as centers of opportunity, leadership, and governance.

Water System Security and Emergency Response Planning

The Washington State Department of Health created this publication to help with emergency response preparedness. It may be downloaded from their Web site, *www.doh. wa.gov/ehp/dw/Security/Publications.htm* or they can be contacted by phone at: (360)236-3162 for questions about water system security.

nesc **7**

NSFC RESOURCES AVAILABLE

To order any of the following products, call the National Small Flows Clearinghouse (NSFC) at (800) 624-8301or (304) 293-4191, fax (304) 293-3161, e-mail nsfc_orders@nesc.wvu.edu, or write NSFC, West Virginia University, PO Box 6064, Morgantown, WV 26506-6064. Be sure to request each item by number and title. A shipping and handling charge will apply.

Small Flows Quarterly Summer 2000, Vol. 1, No. 3

Article "Flood!: Disaster Mitigation for Wastewater Systems" Flooding is the most common type of natural disaster worldwide, accounting for an estimated 40 percent of all natural disasters. High water conditions can be devastating to wastewater treatment systems, especially small systems. A well-thought-out preparation and recovery plan can help get a treatment facility back on line with a minimum of damage and cost. Download from the Web site *www.nsfc.wvu.edu.* **Please note that this issue is only available from our Web site.**

On Tap Magazine, Winter 2002, Volume 1, Issue 4

Security for small drinking water systems is the topic of this issue. Articles include funding sources for preventative steps, crisis communications, the importance of security plans, and things we can learn from international utilities' security measures. Item #DWQUNL04. First copy provided at no charge. The magazine can also be downloaded from the Web site *www. ndwc.wvu.edu.*

For wastewater information, call the NSFC at (800) 624-8301 or (304) 293-4191