Incident Specific Response Checklists

In addition to the above checklists, the following incident specific checklists can be used by DWPs to help guide their response-related activities and tracking of water system status. They are not meant to be all-inclusive. The lists of questions cover general response, natural disasters and security events.

General Response Questions Checklist

1. Record date and time of call, program staff taking the call.
2. Record name of water system and caller, address, phone number, email and PWSID.
3. Record nature of the problem (e.g., date, time, duration, location).
4. Who has been notified (customers, consecutive connections, media, other state agencies, etc.)?
5. What equipment/service has been interrupted/affected?
6. Has water quality been compromised and samples taken?
7. Is alternate water supply needed?
8. Any reports of injury or illness?
9. What actions have been taken so far? Have pre- and post-damage photos been taken?
10. Has the problem been corrected?
11. Is the system a WARN member/has WARN been notified?
12. Is follow-up required? What assistance can the DWP provide?

NATURAL DISASTERS

1. Can the damaged facility be taken offline or system portions isolated?
2. If the system is groundwater, has the well(s) been submerged?
3. Has untreated water (or any contaminant) entered the water system?
4. Has the system lost pressure or have low pressure?
5. Can another facility perform the same function?
6. How long will it take to repair?
7. Do you have power for all components of the water system? Is it from primary power or generator?
   a. If no power:
      i. Do you have a properly sized generator or quick connect capabilities?
      ii. Are there any critical customers served by the system?
      iii. How long have you been without power?
      iv. Who is your power company?
      v. What is the street address of water system operations, or component out of power?
      vi. What is your restricted use plan and storage capacity?

Actions to Be Taken:
- ☐ Utilize proper drinking water advisories for immediate public notice.
- ☐ Provide technical assistance and monitoring advice.
- ☐ Coordinate power outage prioritization for water systems through state EOC.

SECURITY (INTENTIONAL/ACCIDENTAL) INCIDENTS

What type of activity has occurred? Is it physical or cyber; intentional or accidental? The separate checklists below offer targeted questions based on the identified incident type.

Physical Security Incident

1. Is contamination a possible threat to the water system?
2. Is a site characterization being conducted to determine credibility of threat?
3. Have water quality samples been collected for analysis and to confirm contamination incident?
4. Has law enforcement been notified?
5. If site is safe, has the water system and/or law enforcement investigated the facilities and have/can affected components been/be isolated?
6. If the site is not safe, has local hazmat assistance been requested?
7. Has the site and evidence been protected?

Actions to Be Taken:

(Refer to EPA "Water Security Initiative: Interim Guidance on Developing Consequence Management Plans for Drinking Water Utilities" EPA 817-R-08-001, July 2008)

☐ Immediately notify appropriate senior management.

☐ Assist in notifying local law enforcement and the Federal Bureau of Investigation (FBI) for their assistance in investigating the incident.

☐ Coordinate with the DWP's Public Information Officer and water system in issuing a "Water Advisory" notice.

☐ Report incident to the Water Information Sharing and Analysis Center (WaterISAC).

☐ Provide technical assistance and monitoring advice.

Cyber Security Incident

1. What computer systems have been affected and what is the concern?
2. Do you know if the threat is internal (disgruntled employee) or external (computer hacker)?
3. Have computers been disconnected from the internet and staff notified?
4. Has your IT service provider been contacted? Are they analyzing the threat?
5. Is customer information at risk?
6. Does your water system have a SCADA system?
   a. Have any unauthorized changes been made to the SCADA system?
   b. Are water system components and water quality data normal?
   c. Can the SCADA system be taken offline and the water system run manually?

Actions to Be Taken:

☐ Encourage water system to contact their IT service provider for assistance in identifying the threat.

☐ Advise water system to contact law enforcement if a cyber security threat is confirmed.

☐ Assist in reporting the incident to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) ics-cert@hq.dhs.gov,

☐ If appropriate, utilize proper drinking water advisories for immediate public notice.

Chemical Spill Incident

1. Is spill incident accidental or intentional? If intentional, see physical security incident questions as well.
2. When did the spill occur? (date, time, duration, location)
3. What material and how much was spilled?
4. Has the material been contained or what action is being taken?
5. Did any of the materials enter a body of water or source protection area?
6. Who is the primary contact for this spill incident?

Actions to Be Taken:
- ☐ Make sure appropriate State Spill Response Agency and the National Response Center has been contacted.
- ☐ Assist in notification of critical infrastructure and customers in the area.
- ☐ If deemed appropriate, issue proper drinking water advisories for immediate public notice.