

Resolution Relating to the Protocol to Secure Vulnerability Assessments Filed by Water Systems Pursuant to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002

---

**WHEREAS**, In June 2002, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) was signed into law; and

**WHEREAS**, Title IV of this Act amends the Safe Drinking Water Act and outlines actions that every community water system and the U. S. Environmental Protection Agency (EPA) must take to improve the security of the nation's drinking water infrastructure; and

**WHEREAS**, The Bioterrorism Act requires every community water system serving a population greater than 3,300 persons to conduct, certify the completion of, and submit to EPA an assessment of the vulnerability of the system to terrorist attack or other acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water; and

**WHEREAS**, EPA has developed an Information Protection Protocol (Protocol) to safeguard the vulnerability assessments and any information derived from such assessments once in EPA's custody; and

**WHEREAS**, EPA will designate a specially trained person to be the "Information Security Manager" who will administer the protection of vulnerability assessment information and the implementation of the Protocol; and

**WHEREAS**, The Protocol establishes protective measures to

ensure that all vulnerability assessments are kept in a designated area securely locked within its facilities in Headquarters to serve as the Secure File and Review Area accessible only by individuals designated by the EPA Administrator and no information from a submitted vulnerability assessment will be available to anyone other than those designated, except as specified under Sections 1433(a)(6) and (7) of the Safe Drinking Water Act, as amended; and

**WHEREAS**, The Protocol establishes stringent restrictions whereby copying and numbering, loaning, transmitting, and discussing vulnerability assessments is prohibited except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water; and

**WHEREAS**, If the Director of EPA's Office of ground Water and Drinking Water authorizes loaning of a vulnerability assessment(s) to an EPA Regional office, the Region will designate an employee to become the Regional Security Officer who will oversee the implementation of this Protocol and manage all loaned vulnerability assessment(s) at the EPA Regional office level and follow comparable security operations as those implemented centrally in EPA Headquarters by the Headquarters Information Security Manager; and

**WHEREAS**, If the Directory of EPA's Office of Ground Water and Drinking Water determines that an unauthorized disclosure has occurred, or vulnerability assessment information is missing, EPA will notify the affected community water system(s) by written notice containing a description of the incident and the date of disclosure, if known, and the

designated individual who disclosed the information will be subject to criminal prosecution and fines in accordance with provisions of chapter 227, 18 United States Code, applicable to class A misdemeanors, and upon conviction may be imprisoned for not more than one year or both; and

**WHEREAS**, In addition to the foregoing protocol, the National Association of Water Companies Rates and Revenues Committee and Regulatory Law Committee has also prepared a Model Protective Agreement; now therefore be it

**RESOLVED**, That the Board of Directors of the National Association of Regulatory Utility Commissioners (NARUC), convened in its February 2003 Winter Meetings in Washington, D.C., supports the EPA Protocol; and be it further

**RESOLVED**, That Public Utility Commissions, in their review of their information protocol consider the attached Model Protective Agreement prepared by the National Association of Water Companies Rates and Revenues Committee and Regulatory Law Committee; and be it further

**RESOLVED**, That Public Utility Commissions establish comprehensive confidentiality procedures to protect any security related information, the disclosure of which could compromise public safety.

---

Sponsored by the Committee on Water and Ad Hoc Committee on Critical Infrastructure

Adopted by the NARUC Board of Directors February 26, 2003