LAW OFFICES
BRYDON, SWEARENGEN & ENGLAND
PROFESSIONAL CORPORATION
312 EAST CAPITOL AVENUE
P.O. BOX 456
JEFFERSON CITY, MISSOURI 65102-0456
TELEPHONE (573) 635-7166
FACSIMILE (573) 635-3847
E-MAIL: DCOOPER@BRYDONLAW.COM

DAVID V.G. BRYDON
JAMES C. SWEARENGEN
WILLIAM R. ENGLAND, III
JOHNNY K. RICHARDSON
GARY W. DUFFY
PAUL A. BOUDREAU
SONDRA B. MORGAN
CHARLES E. SMARR

DEAN L. COOPER
MARK G. ANDERSON
GREGORY C. MITCHELL
BRIAN T. MCCARTNEY
DIANA C. FARR
JANET E. WHEELER

OF COUNSEL
RICHARD T. CIOTTONE

April 4, 2003

HAND DELIVERED AND SENT BY E-MAIL

Mr. Dale Hardy Roberts
Executive Secretary
Missouri Public Service Commission
Governor State Office Building, 9th Floor
Jefferson City, Missouri 65102
daleroberts@psc.state.mo.us

Re: Protective Order Rule – Proposed Rulemaking
Missouri-American Water Company

Dear Mr. Roberts:

I provide the following comments concerning the propose protective order language on behalf of Missouri-American Water Company.

Missouri-American appreciates the Commission's efforts to increase confidentiality protection for information related to public utility system security by including this as a category of protected materials. Missouri-American encourages the commission to adopt, at a minimum, the proposed treatment for highly confidential and proprietary information, including, in particular, provisions limiting the number of persons who have access to such information, prohibition on copying and the ability to designate material as highly confidential (subject to challenge). Among the three options presented, Missouri-American's preference would be for the document entitled "The Current Two Tiered System Slightly Modified."

However, Missouri-American would also encourage the Commission to consider adopting two exceptions to the provisions which would otherwise require disclosure of highly confidential information, even under the more restrictive highly confidential provisions of the proposed rule. These are as follows:

1. Companies should not, under pain of non-recovery of costs, be required to disclose security-related information that could compromise confidentiality protocols or procedures of other government agencies related to security

information. An example of this type of information is the Vulnerability Assessments which community water systems must develop and submit to the United States Environmental Protection Agency (USEPA) pursuant to the Bioterrorism Act of 2002. Pursuant to that Act, the EPA was directed by Congress to establish protocols for the protection of Vulnerability Assessments that are filed with that Agency. In compliance with this Congressional Mandate, the USEPA issued a Protocol to secure Vulnerability Assessments by community water systems, effective November 30, 2002. The Protocol establishes strict requirements for limiting access to Vulnerability Assessments. A copy of the Protocol is attached for your reference.

Vulnerability Assessments have been and will continue to be the subject of discovery requests in regulatory proceedings. Access to Vulnerability Assessments by any intervenor in regulatory proceedings throughout the United States, even under highly confidential provisions, will severely compromise the USEPA's Information Protection Protocol by providing access to or greatly expanding the range of individuals or entities who can have access to these documents.

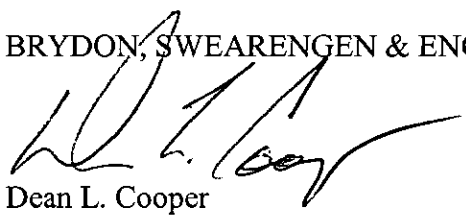
2. Companies should not be required to disclose, under pain of non-recovery of security costs, information that would pose an unacceptable risk of harm to the life, health or safety of persons or the security of the community in general. It should be recognized that there is some information relating to potential plant vulnerability and the capacity to put human life at risk, which simply should not be disclosed during the regulatory process. While the burden should be upon the company to demonstrate that the release of certain information could implicate such serious consequences, the proposed rule should provide an avenue to secure an exemption from release for such information.

These two issues are addressed in a Resolution adopted by the National Association of Regulatory Utility Commissioners (NARUC) on February 26, 2003. In that Resolution, NARUC recognized the Information Protection Protocol EPA issued and urged public utility commissions to establish comprehensive confidentiality procedures to protect any security-related information, the disclosure of which could compromise public safety. The Resolution also included and urged commission consideration of a Model Protective Agreement together with a Summary and Rationale thereof, prepared by the Rates and Revenue and Regulatory Law Committees of the National Association of Water Companies. A copy of the NARUC Resolution is also attached for reference.

Missouri-American Water Company urges the Commission to consider these documents in its deliberations with regard to changes in the treatment of confidential material.

Sincerely yours,

BRYDON, SWEARENGEN & ENGLAND P.C.

By: 

Dean L. Cooper

DLC/tli
cc: Office of the Public Counsel

PROTOCOL TO SECURE VULNERABILITY ASSESSMENTS SUBMITTED BY COMMUNITY WATER SYSTEMS TO EPA

"Information Protection Protocol"

Pursuant to Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002

This Protocol is Effective November 30, 2002

November 30, 2002

EXECUTIVE SUMMARY

In June 2002, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act) was signed into public law (P.L. 107-188). Title IV of this Act amends the Safe Drinking Water Act and outlines actions community water systems and the U.S. Environmental Protection Agency (EPA) must take to improve the security of the nation's drinking water infrastructure. The Bioterrorism Act requires community water systems 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. In turn, EPA is required to handle the submitted vulnerability assessments under strict security arrangements and to develop, by November 30, 2002, in consultation with appropriate federal law enforcement and intelligence officials, the necessary protocols to protect the copies of the assessments.

EPA developed this Information Protection Protocol to safeguard the vulnerability assessments and any information derived from them once these documents are in EPA's custody. This protocol ensures that all assessments are kept in a secure location. Only individuals designated by the EPA Administrator will have access to these documents, and no assessment or "information derived 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.

This protocol builds and expands on EPA's long-standing and excellent track record of handling many types of sensitive information under various environmental statutes and regulations. Throughout the years since EPA's establishment, hundreds of thousands of documents containing sensitive information have been entrusted to EPA. Types of information EPA safeguards include enforcement-confidential information concerning on-going or pending law enforcement efforts, grand jury deliberations, national security information, and information submitted to EPA by regulated business and claimed as confidential. Much of EPA's work involves handling Confidential Business Information (CBI), which contains trade secrets or financial information that if released could harm business interests. EPA has a very stringent training program for protection of such data and uses annual audits and inspections to ensure accountability. No employee has been dismissed for theft of such data.

This protocol establishes a number of protective measures equivalent to those conferred to Secret national security information. The protocol ensures that vulnerability assessments are stored behind closed doors, filed under lock at all times, and accessed only by designated persons under strict security procedures. Vulnerability assessments will be housed at EPA headquarters. A secure review room will be installed and furnished to allow processing of the documents. A document tracking system will allow the vulnerability assessments to be traceable at all times to a single person. Documents will be labeled as sensitive and covered to show that they must be protected. Copying, faxing and loaning of vulnerability assessments will be prohibited except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

An EPA Information Security Manager in headquarters will oversee the protection of the information, manage the day-to-day implementation of the protocol and conduct routine security check-ups. EPA will require a Top Secret clearance for the Headquarters Information Security Manager and a Secret clearance for all other designated individuals. Prior to being designated, potential designees will also undergo security training, and will sign an access agreement which summarizes their responsibilities and personal liabilities if information contained in vulnerability assessments is knowingly or recklessly disclosed. Access will be withdrawn when a designated person terminates employment or no longer requires access because of a change in duties or position. In such cases, the person will be asked to sign a confidentiality agreement prior to termination of access. Each designated person must receive annual refresher security training.

TABLE OF CONTENTS

CHAPTER 1: PURPOSE AND DEFINITIONS

1.1 Purpose of this Protocol

This "Protocol to Secure Vulnerability Assessments Submitted by Community Water Systems to EPA" or Information Protection Protocol, describes the policies and security procedures put in place by EPA to protect from unlawful access and use the copies of vulnerability assessments to be submitted by community water systems.

This protocol is intended to serve as the security manual for individuals to be designated by the EPA Administrator to have access to the vulnerability assessments. It may also inform community water systems as to how EPA will protect and secure their vulnerability assessments.

1.2 Protocol Updates and Revisions

If procedures change for the control, storage, security and handling of vulnerability assessments submitted by community water systems, EPA will update the relevant pages in this protocol and distribute a revised protocol to all designated individuals.

1.3 Definitions

Authorized Access List: A list of those people who the EPA Administrator has designated for access to vulnerability assessments per section 1433 of the Safe Drinking Water Act. Includes the names of the designated individuals, the date of designation, and the date their annual refresher training is due.

Certification: Written notification sent by community water systems to EPA upon completion of a vulnerability assessment required by section 1433(a)(2) of the Safe Drinking Water Act.

Community Water System: As defined in the Safe Drinking Water Act, a community water system is a public water system that (a) serves at least 15 service connections used by year-round residents of the area served by the system, or (b) regularly serves at least 25 year-round residents. The term is generally used in this document to refer to those systems serving a population greater than 3,300 persons that are required to conduct, certify the completion of, and submit to EPA a copy of their vulnerability assessment per section 1433(a)(2) of the Safe Drinking Water Act.

Designated Person or Designee or otherwise authorized individuals: A designated person or designee is an individual designated by the EPA Administrator to have access to vulnerability assessment(s) in accordance with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. An otherwise authorized individual is a person to whom a designated individual is authorized to provide access to vulnerability assessment information under Sections 1433(a)(6) and (7) of the Safe Drinking Water Act.

Information contained in or derived from a Vulnerability Assessment: Information originating from a submitted vulnerability assessment or information generated by EPA as a result of reviewing and analyzing submitted vulnerability assessments.

Information Security Manager: EPA Office of Ground Water and Drinking Water employee in Headquarters assigned to oversee the protection of vulnerability assessment information and implementation of this protocol.

PWSID#: Public Water System Identification Number used by states and EPA in their drinking water regulatory programs.

Regional Security Officer: EPA employee in an EPA Regional office assigned to manage loaned vulnerability assessments and implement this protocol on a regional level.

Vulnerability Assessment or VA: As required under section 1433(a) of the Safe Drinking Water Act, a review of certain specified items to assess the vulnerabilities of the community water system to terrorist attack or other intentional act intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. The submitted vulnerability assessment must include, but is not limited to, a review of the following parts of a water system: pipes; constructed conveyances; physical barriers; water collection, pre-treatment, treatment; storage and distribution facilities; electronic, computer or other automated systems; use, storage or handling of chemicals; and system operation and maintenance.

Vulnerability Assessment Information: Used to refer to both vulnerability assessments submitted to EPA and information contained in or derived by EPA from a submitted vulnerability assessment.

Vulnerability Assessment (VA) Tracking Number: Number assigned by EPA to a certification, vulnerability assessment, and information derived from a particular vulnerability assessment, for purposes of tracking its receipt and internal handling. This number may be the PWSID#.

CHAPTER 2: MANDATORY PROTECTIVE MEASURES

EPA will observe the following protective measures in location(s) where vulnerability assessments are kept and secured.

2.1 Receipt and Tracking

A designated individual will transfer vulnerability assessment packages to the Secure File and Review Area where they will be date stamped, covered, marked, assigned a Vulnerability Assessment Tracking Number, and securely filed. EPA may use barcodes for file management and tracking. For each vulnerability assessment, EPA will produce a "File Out" tag that includes the name of the Community Water System, the address, and PWSID# (Exhibit A). EPA will acknowledge receipt of the assessment to the water utility.

2.2 Cover Sheets for Vulnerability Assessment Information

EPA will affix to all vulnerability assessment information a cover sheet (Exhibit B) to distinguish it from other documents.

2.3 Markings to Identify Vulnerability Assessment Information

EPA will mark all vulnerability assessments and any sensitive documents produced in the course of analyzing the vulnerability assessments, with a stamp to identify the sensitivity of the information and as EPA's copy of the vulnerability assessment (Exhibit C). The stamp must be placed on the front of the first page (or on the cover, if the document has one) and on the back of the last page (or back cover, if the document has one). Additionally, EPA may mark other pages as necessary.

2.4 Secure File and Review Area

EPA will designate an area within its facilities in Headquarters to serve as the Secure File and Review Area. Designated individuals will open and process vulnerability assessments in this area only. Only designated individuals will have electronic pass cards and door combinations to grant access to this area. The area will have a secure door with a secure doorframe and doorjamb. As much as possible, EPA will locate this area within already-existing protected areas. EPA may consider the use of intrusion alarms and monitoring cameras as an alternative or in addition to having the Secure File and Review Area within already-protected areas. EPA will place a sign outside the area to clearly convey that only authorized access is permitted.

EPA will furnish the Secure File and Review Area with individual workstations, desk(s), stand-alone computers, chairs, document shredders, electronic date/time stampers, and other supplies as may be necessary.

There may be times when a non-designated individual needs to enter the Secure File and Review Area directly escorted by a designated individual. For example, stand-alone computers may need repair, or the room may need to be cleaned. In such circumstances, a designated individual must ensure that no vulnerability assessment information lies exposed on tables or workstations and that the visitor signs-in upon entry, records his/her contact information, and signs-out upon departure. Designated individuals will accompany non-designated individuals at all times while in the secure area.

2.5 Storage Equipment

EPA may use two types of containers to store vulnerability assessments: metal file cabinets with locking bars and three-way changeable combination locks, or GSA-approved Class 6 security containers used for storing national security information.

2.6 Custody Rules

The authorized recipient of a vulnerability assessment will acknowledge receipt by completing an entry on the "File Out" tag belonging to the particular vulnerability assessment. The entry must contain the printed name, signature, date removed, and time of removal. When returning the document to the file cabinet, the recipient must indicate the date returned, and initial the entry. Refer to Exhibit A for a sample file activity log. When not in use, documents must be returned to the locked file cabinets. EPA will use the individual vulnerability assessment "File-out" tags to trace the custody of documents.

2.7 Copying Restrictions and Numbering

EPA will not copy vulnerability assessments except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

If and when the Office Director authorizes copying, EPA will prepare a watermarked paper and copy the document using this paper to distinguish the copy from the original document submitted by the community water system. EPA will number each copy, track it, cover it and protect it in the same fashion as the submitted vulnerability assessment.

2.8 Loaning Vulnerability Assessments to EPA Regional Offices

EPA Headquarters will not loan vulnerability assessments to Regional offices except on a rare, case-by-case basis as authorized by the Director of the Office of Ground Water and Drinking Water.

If and when the Office Director authorizes a loan to a Regional office, an EPA designated individual in the Regional office will fill out a loan request (Exhibit D), and a

Headquarters designated individual will make a single copy of the vulnerability assessment and transfer it to the Region following the transmittal procedures described below. Both the Headquarters and the Regional designated individuals will retain a copy of the loan request. Loans will be time-limited and extensions may be requested. When a loan expires, EPA Headquarters will obtain the materials back from the EPA Regions. EPA Regions will not be authorized to make copies or keep any sensitive materials. EPA Regions with loaned vulnerability assessments must set in place comparable protective measures as described herein.

2.9 Hard Copy Transmissions

EPA will not transmit hard copies of vulnerability assessments except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

If and when the Office Director authorizes a hard copy transmission, EPA will double-wrap all materials and write the recipient's name and the statement "Sensitive Vulnerability Assessment Information—To be Opened by Addressee Only" in the inner envelope. The outer envelope will only contain the name and address of the recipient, and the direct return address, and be free of any indications that the package contains sensitive vulnerability assessment information.

EPA will send the document using tracked mail such as certified mail, hand-delivery, or other secure method. EPA will require return receipt if certified mail is used. If hand-delivery is used, the carrier must be a designated individual. EPA will not permit the transfer of vulnerability assessments using regular first class mail.

The sender will include a receipt inside the package identifying the contents of the package. The recipient will sign the receipt and send it back to the sender within five days of receipt, to verify receipt and contents. The sender will retain all receipts received for auditing. The sender must also obtain a receipt from the courier service employee who picks up the package.

2.10 Fax Transmissions

EPA will not transmit vulnerability assessments by fax except on a rare, case-by-case basis as authorized by the Director of EPA's Office of Ground Water and Drinking Water.

If and when the Office Director authorizes a fax transmission, EPA will use only fax machines with secured lines.

2.11 Discussing Vulnerability Assessment Information on the Telephone

Designated or otherwise authorized individuals may discuss vulnerability assessment information on the telephone only if the transfer of information can not be accomplished in person. In such circumstances, designated individuals should use an encrypted telephone line if available. Under no circumstances may designated persons leave messages containing vulnerability assessment information on voice mail.

2.12 Use of Electronic Mail (E-Mail)

EPA does not authorize the use of email or any other electronic mail system to transmit vulnerability assessment information.

2.13 Use of Tele-Video Conferences

EPA headquarters and EPA regional offices may display and discuss vulnerability assessment information during tele-video conferences. All attendants must be designated or otherwise authorized individuals. If available, compressed video encryption will be used.

2.14 Protecting Information Derived from Vulnerability Assessments

EPA will protect information derived from submitted vulnerability assessments in the same fashion as submitted vulnerability assessments.

2.15 New Non-Sensitive Records

In the course of conducting work activities relating to drinking water security, designated individuals and other EPA staff may obtain information, such as briefing documents, on drinking water system vulnerabilities that have not been derived from the vulnerability assessments submitted to EPA. For example, a designated individual may attend a conference or a workshop and be voluntarily handed information related to water security. EPA staff may also take notes on such presentations. EPA will consider these records, such as handouts and notes, to be personal working papers that need not be protected as strictly as submitted vulnerability assessment information.

2.16 Use of Stand-Alone Computers

Designated individuals may not use computers connected to EPA networks or the Internet, but may use stand-alone computers in the Secure File and Review Area to track submission of the certifications and aggregate data to conduct analysis of vulnerability assessments. There will be no electronic version of vulnerability

assessments, and no information derived from vulnerability assessments will be kept in electronic systems with public access.

2.17 Use of Home Computers

EPA will not authorize the use of home computers in connection with vulnerability assessment information.

2.18 Discussing Sensitive Vulnerability Assessment Information in Meetings

A check to determine that all meeting participants have been designated will precede any discussion of information pertaining to vulnerability assessments. The chair of any meeting that involves a discussion of vulnerability assessment information must ensure that only designated or otherwise authorized individuals are present. At the close of the meeting, the chair of the meeting must ensure all sensitive information, including materials produced at the meeting, is secured.

2.19 Periodic Security Reviews

The Headquarters Information Security Manager (and Regional Security Officers in EPA Regions where vulnerability assessments are on loan) will conduct periodic security inspections/reviews to ensure security practices are being followed. Those who conduct the security reviews will promptly document the results and share them with the Director of EPA's Office of Ground Water and Drinking Water or his/her delegate.

2.20 Disposition of New Sensitive Records

EPA will destroy by shredding, pulverizing or burning, any dated or no longer needed sensitive documents produced in the course of analyzing the vulnerability assessments consistent with EPA's obligations under the Federal Records Act.

CHAPTER 3: DESIGNATIONS AND AUTHORIZED ACCESS PROCEDURES

3.1 Designator

The Bioterrorism Act authorizes the EPA Administrator to designate those individuals who will have access to the vulnerability assessments.

3.2 Selection of Designated Persons

The EPA Administrator will designate those individuals determined to need access to the vulnerability assessments. The EPA Assistant Administrator for Water and the EPA Regional Administrators will identify individuals to be designated based on the following criteria:

- Role in handling and reviewing the vulnerability assessments, and implementing the Bioterrorism Act; and
- Knowledge of community water systems and vulnerability assessment methodologies.

An EPA employee may decline designation.

3.3 Basic Responsibilities of Designees

Every designated person must protect and safeguard any vulnerability assessment information at all times and in compliance with this protocol, not discuss sensitive information with anyone who is not a designated individual or otherwise authorized under Section 1433, and promptly report any apparent violation of access to the Headquarters Information Security Manager.

EPA recognizes that situations not covered by this protocol may arise. In such cases, the Headquarters Information Security Manager will be available for guidance, and each designated person will ensure through personal conduct and accountability that he or she will act consistently with these guidelines to protect, to the best of his or her ability, all vulnerability assessment information.

3.4 EPA's Headquarters Information Security Manager

EPA will assign a designated person to be the **"Information Security Manager."** This person will oversee the protection of vulnerability assessment information and the implementation of this protocol. The Headquarters Information Security Manager will:

- Be the focal point for protection of community water system vulnerability assessment information in EPA
- Maintain the Vulnerability Assessment Tracking System

- Arrange and conduct security briefings of potential designees, and conduct refresher training
- Issue and safeguard the original signed Access Agreements
- Maintain an updated Authorized Access List of designated persons
- Conduct periodic announced and unannounced security inspections for conformance with this protocol, and investigate any reported breaches of security
- Approve contractor security plans in consultation with the appropriate EPA Contract Project Officer, if applicable
- If needed, oversee the vulnerability assessment loan system and keep a record of the loan requests

3.5 EPA's Regional Security Officers

If the Director of EPA's Office of Ground Water and Drinking Water authorizes loaning a vulnerability assessment(s) to an EPA Regional office, the Region will assign a designated employee to become the **"Regional Security Officer."** This person will become the focal point for management of 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. Regional Security Officers will have the following responsibilities:

- Be the focal point for protection of loaned vulnerability assessments at the Regional level
- Oversee the implementation of this protocol among designated individuals
- Maintain an updated record of all designated persons within the Region, to update the official Authorized Access List
- Arrange and conduct security briefings of potential designees in the Region, in consultation with the Headquarters Information Security Manager, and conduct refresher security training
- Conduct security inspections periodically, in consultation with the Headquarters Information Security Manager
- Respond to Headquarters Information Security Manager requests.

3.6 Steps in the Designation Process

Step 1: Identification of Potential Designees

The EPA Assistant Administrator for Water and the EPA Regional Administrators will identify individuals to be designated based on the criteria in section 3.2 of this Protocol.

Step 2: Investigation of Potential Designees

EPA will require a Top Secret clearance for the Headquarters Information Security Manager and a Secret clearance for all other designated individuals, including any Regional Security Officers.

The EPA Administrator may designate individuals pending completion of their security clearance process. Temporary designations will be withdrawn if designated individuals do not complete the clearance process successfully.

Step 3: Security Training and Evaluation

The Headquarters Information Security Manager (or the Regional Security Officer) will train potential designees on the Bioterrorism Act and the procedures described in this protocol. At this time the potential designee will obtain a copy of this protocol. The Headquarters Information Security Manager may ask the potential designee several questions to reinforce the material and ability to implement this protocol.

Step 4: Access Agreement

After successful completion of the security training, the potential designee will sign an Access Agreement (Exhibit E) indicating an understanding and acceptance of the terms and responsibilities. The Headquarters Information Security Manager will also sign the Access Agreement to indicate the designated person was trained and understands the material conveyed. If the designated person is an EPA employee, the direct supervisor of the designated person also signs the Access Agreement.

Step 5: Designation

Designation is effective upon the EPA Administrator's official recognition of the individual as a designated person in the form of a signed Memorandum. Upon designation, the Headquarters Information Security Manager will add the persons' name to the Authorized Access List. The list will be used to control access to the vulnerability assessment information and includes the names of designated individuals, the date of designation, and the date their annual refresher training is due.

3.7 Annual Refresher Training

Each designated person must receive an annual refresher training.

3.8 Use of Contractors

If EPA enters into a contractual relationship in order to carry out its mandate under the Bioterrorism Act, and contract employees need to be designated, these employees will be required to follow EPA procedures and implement this protocol as any designated

individual. As described above, EPA will also require a Secret level clearance for contractors.

3.9 Removal of Designation or Termination of Access

EPA will withdraw designations when the individual no longer requires access to vulnerability assessments because of a change in duties or position. An individual may also be withdrawn, for example, if found not to be adhering to security procedures, or if he or she fails to attend the annual security training. Prior to the designation being relinquished or withdrawn, the designated individual must complete the "Confidentiality Agreement for Termination of Access" (Exhibit F) in accordance with the "Access Agreement" signed prior to designation, and return to the Headquarters Information Security Officer any electronic entry cards to the Secure File and Review Area.

CHAPTER 4: REPORTING AND INVESTIGATION OF VIOLATIONS OF PROCEDURES, LOST DOCUMENTS AND UNAUTHORIZED DISCLOSURES

4.1 Introduction

All designated individuals must report possible violations of security procedures, the loss or misplacement of vulnerability assessment information, and any unauthorized disclosure of materials immediately to the Headquarters Information Security Manager.

For designated EPA employees, the security procedures in this protocol are enforceable by disciplinary actions, set forth in this chapter, in addition to criminal penalties. For designated non-EPA employees, only criminal penalties are enforceable per section 1433 of the Safe Drinking Water Act.

4.2 Verbal Reporting

Any designated individual (EPA employee or not) should provide verbal notice to the Headquarters Information Security Manager within one working day if it is possible that

- Security procedures have been violated
- Vulnerability Assessment materials have been lost or misplaced
- A non-designated person who is not otherwise authorized under Section 1433 has obtained access to vulnerability assessment information.

4.3 Written Reporting

Within two working days, any designated individual (EPA employee or not) should follow up the verbal report with a written report. The written report must describe the possible violation of procedures, the unauthorized disclosure of information, and the materials believed lost or misplaced. It must also include a description of any relevant circumstances or facts known by the designee.

The designee may examine files and discuss the matter with the Headquarters Information Security Manager or the Regional Security Officer. However, only the Headquarters Information Security Manager will be authorized to conduct interviews, review logs, and carry out a detailed investigation.

4.4 Review and Investigation of Written Report

The Headquarters Information Security Manager will inform the Director of EPA's Office of Ground Water and Drinking Water if an incident has occurred. The Office Director will then assign an individual to investigate the incident and to determine if a violation of procedures, loss of information or unauthorized disclosure has occurred.

If the investigation reveals any evidence of a knowing and reckless disclosure of vulnerability assessment information, the Office Director will immediately refer the matter to the appropriate individuals.

4.5 Notification to Affected Community Water System

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

4.6 Disciplinary Action for EPA Designees Only

[Reserved.]

4.7 Criminal Penalties for EPA and non-EPA Designees

The Director of EPA's Office of Ground Water and Drinking Water will notify the appropriate individuals if a designated person knowingly or recklessly releases or discloses vulnerability assessment information to any unauthorized person. The designated individual who disclosed the information is 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. A convicted EPA employee will also be removed from Federal office or employment.

APPENDIX A: The Public Health Security and Bioterrorism Preparedness and Response Act of 2002

In June 2002, the President signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Bioterrorism Act). Title IV of this Act amends the Safe Drinking Water Act (SDWA) by adding new sections 1433 through 1435 which outline actions community water systems and the U.S. Environmental Protection Agency (EPA) must take to improve the security of the nation's drinking water infrastructure. For Title IV of the Bioterrorism Act, consult Public Law 107-188.

Actions required of Community Water Systems

The Bioterrorism Act requires each community water system serving a population greater than 3,300 persons to conduct an assessment of the vulnerability of its system to a terrorist attack or other intentional acts intended to substantially disrupt the ability of the system to provide a safe and reliable supply of drinking water. A vulnerability assessment must include but is not limited to a review of certain specified items (e.g., pipes; constructed conveyances; physical barriers; water collection, pre-treatment, treatment; storage and distribution facilities; electronic, computer or other automated systems; use, storage or handling of chemicals; and system operation and maintenance).

After completion of each vulnerability assessment, each community water system must certify to the EPA Administrator that the assessment has been conducted, and submit a written copy of its assessment to EPA. These requirements are phased-in depending on the size of the community water system.

POPULATION SERVED BY COMMUNITY WATER SYSTEM	DEADLINE FOR CERTIFYING AND SUBMITTING VULNERABILITY ASSESSMENT
100,000 or more persons	March 31, 2003
50,000 to 99,999 persons	December 31, 2003
3,301 to 49,999 persons	June 30, 2004

Small community water systems serving a population of 3,300 or less persons are to be provided guidance by EPA on how to conduct a vulnerability assessment, among other things. However, small systems are not required to prepare a vulnerability assessment or submit it to EPA.

Actions required of EPA

EPA is required to handle all submitted information under strict security arrangements and to develop protocols as may be necessary to protect the copies of the assessments and information derived from the assessments, from unauthorized disclosure. The protocols must be developed prior to November 30, 2002, in consultation with appropriate federal law enforcement and intelligence officials.

The protocols must ensure that: (a) each vulnerability assessment is kept in a secure location; (b) only individuals designated by the EPA Administrator have access to these vulnerability assessments; and (c) no vulnerability assessment or part of an assessment, or information contained in or derived from an assessment, is available to anyone other than the designated individuals, with some exceptions noted below.

Designations, FOIA exemption, and disclosure considerations

The Bioterrorism Act authorizes the EPA Administrator to designate those individuals who will have access to the copies of the vulnerability assessments submitted to EPA. Generally, only these individuals may have access to this information, and no copy, part or information contained or derived from a vulnerability assessment will be generally available to anyone other than those designated by the Administrator.

Information provided to EPA under section 1433 and any information derived therefrom, is exempt from disclosure under the Freedom of Information Act, or FOIA, Title 5 United States Code section 552. The only exception is for information that specifies the system submitting the certification and the date of the certification.

Furthermore, the Bioterrorism Act addresses the situation where a state or local FOIA requirement could be 'triggered' by submission of a written copy of vulnerability assessment to EPA. The Act provides that no community water system will be compelled to submit a copy of its assessment to any governmental entity occasioned by the requirement that the system submit such an assessment to EPA.

The only allowed exceptions for disclosure of vulnerability assessment information by designated individuals is for use in any administrative or judicial proceeding to impose a penalty for failure to comply with the security provisions, and for specific actions under identified sections of the Safe Drinking Water Act; namely, sections 1445 (records and inspections) and 1431 (emergency powers). In addition, no information may be withheld from Congress or from any committee or subcommittee of Congress.

Designated U.S. government employees may discuss the contents of a vulnerability assessment with a state or local official.

Personal liabilities and penalties

Any *designated* person who knowingly or recklessly reveals vulnerability assessment information is 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. A convicted employee will also be removed from Federal office or employment.

APPENDIX B: EPA's Experience in Protecting Sensitive Information

Since the establishment of the Agency in December 1970, hundreds of thousands of documents containing sensitive information have been entrusted to EPA.

Under the Clean Water Act, EPA protects confidential trade secret data on the production, treatment and discharge of wastewater. Approximately 10,000 records over the past 10 years have gone through EPA's Office of Water security program. Only a few records have been reported missing and after extensive investigation in each case, the Agency concluded that there was a high probability of their having been destroyed. Following these instances, immediate corrective measures were taken, including the requirement of monthly reports to track all Confidential Business Information (CBI) transmittals.

Various other environmental statutes and regulations provide a framework for EPA to protect sensitive information, including:

- Toxic Substances Control Act (TSCA): protects CBI on chemical formulas for new and existing chemical products, the volume of chemicals produced, industrial processes used to make particular substances, and financial information about chemicals a company plans to produce;
- Resource Conservation and Recovery Act (RCRA): protects information about the content of waste streams which could potentially be used by competitors to determine what substances a company manufactures;
- Comprehensive Environmental Response, Compensation and Liability Act (CERCLA or Superfund) and the Emergency Planning and Community Right-to-Know Act (EPCRA): secures information about emergency planning and hazardous chemical inventories;
- Federal Insecticide, Fungicide and Rodenticide Act (FIFRA): safeguards chemical formulas, production volume as well as health and safety data about pesticides;
- Clean Air Act (CAA): protects emission production and consumption data, information from engine manufacturers, sales volumes by vehicle class, and information relating to fuel or fuel additive registrations.

The volume of information handled and kept secure by EPA in TSCA alone is significant: 5370 original submissions containing TSCA CBI were processed in Fiscal Year 2001. A total of 145,000 documents (originals and copies) are currently on file under this program. There is also a significant microfiche collection probably numbering in the hundreds of thousands of individual fiche. Approximately 1500 persons including EPA, contractors, and other Federal agencies' employees have access to FIFRA CBI and our track record for securing FIFRA sensitive information is unblemished. There have been no reported cases of compromise in the thousands of documents that are handled weekly under FIFRA. The Agency has a very stringent training program for protection of such data and annual audits and inspections ensure accountability. No employee has been dismissed for theft of such data and very few disclosures or releases of such information to outside sources have occurred. In the late 1970's, EPA's procedures for protecting TSCA CBI were closely scrutinized when the Polaroid Corporation challenged

EPA's potential disclosure of chemical formulations (Polaroid Corporation v. Costle, 11 Envir. Rep. Cas (BNA) 213 (D. Mass 1978)). In response, EPA agreed to adopt new rules for protecting TSCA CBI, and the U.S. District Court of the District of Massachusetts subsequently issued a Consent Order that required EPA to implement an enhanced system for tracking the information, among other actions.

NARUC

Serving the consumer interest by seeking to improve the quality and effectiveness of public utility regulation in America.

Home

About NARUC

Congressional Testimony

ERRA Website

Meetings

NARUC Programs

Resolutions

Resources

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. Evironmental 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 vulnerabilty 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

NAWC Regulatory Law Committee & Rates & Revenue Committee

Model Protective Agreement

Summary & Rationale

On several occasions NARUC has expressed concern about the confidentiality of security-related information during the regulatory process. The water industry shares this concern. In its Resolution adopted November 13, 2001 NARUC noted that, due to the tragedy of September 11, 2001, a heightened focus has been placed upon Public Utility Commission procedures related to cost recovery and handling of sensitive documents and it encouraged Commissions and water utilities to work together to identify effective procedures for selective access to information related to security measures of a highly sensitive nature which, if accessible to the public, could conceivably compromise security and service reliability.

In its resolution of March 14, 2002, NARUC specifically noted that current procedures and state statutes outlining the treatment of confidential information were developed primarily in the context of financially or competitively sensitive issues, and that they may not adequately address the need for differential treatment in handling security sensitive materials.

Concern about public access to security-related information during the regulatory process has recently increased as a result of the issuance, by the USEPA, of its Protocol to Secure Vulnerability Assessments by Community Water Systems to EPA ("Information Protection Protocol"), effective November 30, 2002. Pursuant to the Bioterrorism Act passed by Congress in 2002, community water systems must perform vulnerability assessments of their systems and submit those assessments to the USEPA. The EPA was directed by Congress to establish protocols for the protection of vulnerability assessments that are filed with that agency. The Information Protection Protocol addresses this mandate. The protocol establishes strict requirements for limiting access to vulnerability assessments including:

- Limiting access to assessments to a very small number of designated individuals under strict security procedures
- Prohibitions on copying, faxing or even lending assessments to other divisions within the USEPA
- Restricting telephone or other discussions of assessment information and unconditionally prohibiting transmission of it
- Requiring security clearances for persons who do have access as well as security training
- Criminal penalties under federal law for violations provisions
- Numerous other provisions

Vulnerability Assessments required by the Bioterrorism Act already have been and will continue to be the subject of discovery requests in regulatory proceedings. This raises the very distinct possibility that the purposes of the Bioterrorism Act and the EPA Information Protection Protocol will be severely compromised by providing public access to or greatly expanding the range of individuals or entities (i.e., any staff or intervenor in a proceeding) that will have access to these sensitive documents. Congress and the

EPA are obviously of the opinion that access to these documents could severely compromise public safety and have taken precautions to strictly limit that access accordingly. Utilities and utility commissions should be equally concerned that regulatory procedures not be utilized to the detriment of public safety. This concern, however, extends to other security-related information in addition to vulnerability assessments, such as specific security measures, engineering drawings, points of vulnerability or documents from which such information could be obtained, which could pose equal or greater risks to public safety.

For these reasons, consistent with NARUC's expressed recognition that existing procedures for the treatment of confidential information involving financial and competitive issues may not adequately address the need for differential treatment of security materials, the NAWC Law and Rates and Revenues Committees have put together a Draft Protective Agreement for Discussion Purposes. The Draft Protective Agreement is intended to facilitate discussion of these important issues and to suggest one possible protocol for accommodating the legitimate needs of all the participants in the regulatory process.

In sum, the Protective Agreement:

- Places security-related information in a special category and allows the utility to initially claim protection for all such material
- Allows staff and any party who signs the Protective Agreement to view security-related material and then allows any such parties to challenge the Protective status of any specific information
- Initially restricts the number of individuals who will have access to the information, but provides a mechanism for additional individuals to be added for good cause, on a need to know basis, and where public safety would not be compromised
- Restricts copying and certain use of the information, but allows challenges to these restrictions
- Does not require disclosure of documents, such as vulnerability assessments, that would compromise protective protocols of other government agencies, or pose an exceptional risk to public safety

In a post 9/11 world, we believe the Draft Agreement reflects a reasonable compromise between the need to protect public safety and the legitimate needs of staff, intervening parties and the public to information concerning security issues in regulatory proceedings. The Draft Agreement involves a number of, but not all, the approaches reflected in the EPA Information Protection Protocol. We hope this document will stimulate further discussion and help to ultimately resolve these issues consistent with the public interest.

NAWC Regulatory Law Committee & Rates & Revenue Committee

Model Protective Agreement
for Discussion Purposes

1. Purpose & Construction

A. The primary purpose of this Protective Agreement ("Agreement") is to protect public health and safety by preventing unauthorized access to or release of documents and other information disclosed during the regulatory process with regard to security measures and related costs. Consistent with this purpose, the Agreement provides an opportunity for protected review by authorized representatives of Staff and Intervenors ("Parties") of documents and other information with regard to security measures and related costs, which is reasonably necessary for effective regulatory review. The Agreement provides a mechanism for utilizing such information in regulatory proceedings, while protecting the information from improper disclosure which could compromise or impair effectiveness of the security measures and thereby potentially jeopardize public health and safety. This Agreement shall be construed, and any disputes hereunder resolved, consistent with the primary purpose to protect public health and safety.

B. The Company may initially designate all documents or information concerning security measures and related costs as "Protected Materials". Pursuant to the protections afforded herein, Authorized Representatives will have the opportunity to review Protected Material and an opportunity to challenge the Company's designation of any particular documents or information as "Protected Materials".

2. Definitions

A. "Protected Materials" means documents and information, in any form, and/or tangible items pertaining to security measures and related costs, including but not limited to, responses to data requests related thereto.

B. "Authorized Representatives" means, in respect to the Commission staff, one counsel of record and one other staff member or person under contract to the staff, each authorized in writing by a senior official of the Commission to have access to Protected Materials. In regard to any other party, "Authorized Representatives" means a single counsel of record and a single other person, employed by or under contract to the party, each authorized by the party to review "Protected Materials", provided such authorization is evidenced to the Company by a written certification by the party which is mutually agreeable to the parties.

With the consent of the Company, staff and any other party may add additional Authorized Representatives. Staff and any other party may also file a motion seeking to add additional Authorized Representatives. Designation of all Authorized Representatives shall be on a "need to know" basis. Motions to add additional Authorized Representatives shall state with specificity why such individuals are necessary to effective review of Protected Materials, the qualifications of proposed individuals to review such materials, and why the additional Authorized Representatives will not increase the risk of public disclosure of Protected Materials which could adversely affect public health and safety. The Commission/ALJ may allow additional Authorized Representatives only upon motion, with a finding that such additions are necessary for effective review of such expenditures and that such additions will not increase the risk of public disclosure of Protected Materials.

C. "Intervenor" means an intervenor in this proceeding.

3. Access to Protected Materials

A. The company shall provide access by an Authorized Representative to Protected Materials only after such Authorized Representative has executed a non-disclosure certificate to this Agreement. Except with consent of the Company: (i) access shall be at the offices of the company and under the supervision of the company; (ii) Protected Materials shall not be removed from the offices of the company; and (iii) no copies shall be provided to an Authorized Representative except as provided herein. Authorized Representatives may make notes or memoranda from a review of the "Protected Materials" and may remove such notes and memoranda. In all other respects such notes and memoranda shall remain Protected Material and subject to the provisions hereof. The Protected Materials shall be used only to assist Commission staff or any other party to prepare for or to try this proceeding and shall not be used for any other purpose in this or any other jurisdiction.

B. Notwithstanding any provision of this Order, the Company may deny or further limit access, as necessary, to documents or information the disclosure of which would constitute a serious, unacceptable risk of harm to the life, health or safety of persons or the security of the community in general, or which could compromise confidentiality protocols or procedures of government agencies related to security information. The Company shall identify any such documents with specificity and clearly describe why access to such documents should be denied.

4. Non-Disclosure

Except as provided in this Agreement, The contents of Protected Materials to which the Commission staff or other party is given access, and any notes, memoranda or any form of information or opinions regarding or derived from the Protective Materials shall not be disclosed to anyone other than an Authorized Representative in accordance with this Order; except that an Authorized Representative may disclose his or her conclusions or findings solely within, and for the purposes of, this proceeding and in accordance with this Order. The Protected Materials shall not otherwise be published, disclosed or divulged except as expressly provided herein. The Commission staff, and any other party shall treat all notes and memoranda or opinions regarding or derived from the Protected Materials as highly confidential and the contents of Protected Materials and any information derived from them shall be considered confidential, and shall not be deemed public records. The Commission staff, any party, the Administrative Law Judge or the Commission may discuss any position or conclusion regarding security expenditures and testimony in Briefs, Orders, Pleadings, or hearings in this proceeding in accordance with this Agreement.

This Agreement or production of any document pursuant to this Agreement shall not constitute a waiver of any privilege or other basis for objecting to disclosure or seeking limitations on disclosure.

5. Dispute Resolution

Should an Authorized Representative reviewing or receiving any Protected Materials under this Agreement believe that the information should not be accorded confidential protection pursuant to this Agreement, or that access to any particular document or information should not be denied, he/she shall inform the company thereof and the company and the Authorized Representative will attempt to negotiate a satisfactory resolution of the issue. If a satisfactory resolution is not achieved, the information in dispute shall continue to be maintained as Protected Materials in accordance with this Order, but the Authorized Representative shall inform the company in writing, electronically or otherwise, that the Authorized Representative believes the information in dispute should not be afforded confidential treatment, or why access should be permitted. In the event the company maintains that the information in dispute should be accorded confidential treatment or access denied, the Authorized Representative may file a Motion seeking a determination that the information in dispute should not be afforded confidential treatment pursuant hereto or that access should be permitted, subject to the protections hereof. Any such Motion shall identify with specificity the disputed information, why such information should not be accorded confidential treatment or access denied and why public disclosure of the subject information will not impair the effectiveness of such

measures and thereby potentially jeopardize public health and safety. The Commission/ALJ may grant such Motion if it finds that public access to and disclosure of such information will not adversely affect public health and safety.

After a review of the Protected Materials, an Authorized Representative may make a written request electronically or otherwise for copies of specific Protected Materials and the Company and the Authorized Representative will attempt to resolve such requests in good faith. In the event the company and the Authorized Representative are unable to resolve the issue, the Authorized Representative may file a Motion seeking an Order requiring the Company to provide copies of specific Protected Materials. Any such Motion shall state with specificity why provision of such copies is necessary for effective review of Protected Materials and why provision of copies will not increase the risk of public disclosure of Protected Materials which could adversely affect public health and safety. The Commission/ALJ may require the company to provide an Authorized Representative with requested copies if it finds that the provisions of such copies is necessary for effective review of the Protected Material and will not increase the risk of public disclosure of Protected Materials which could adversely affect public health and safety. Any such copies shall also be considered Protected Materials and subject to all the provisions hereof.

Any motion filed under this Section 5 shall be subject to the provisions of Section 10 hereof.

The Parties hereto agree that remedies at law may be inadequate to protect the Company in the event of a breach of this Agreement and the Company may seek injunctive relief in favor of the Company to prevent the continuation of any such breach without proof of actual damages and staff and any party shall not unreasonably oppose the Company's request for injunctive relief.

6. Receipt and Tracking

As part of its designation of Authorized Representatives, the Commission staff and any party shall also designate an individual whose responsibility it is to insure compliance with this Protective Order, and who will acknowledge receipt of any Protected Materials. Within one month from the conclusion of this proceeding or any judicial review proceedings involving security related expenditures, the Commission staff and any party will return any Protected Materials, any notes or memoranda related thereto and any copies thereof to the company. Any electronic copies of Protected Materials made by Authorized Representatives shall be eliminated.

The Company may appeal any Order requiring disclosure of Protected Materials to the Commission or the courts, according to law, and during any appeal process the Protected Materials shall maintain their protected status pending final resolution of said appeals.

7. Maintenance of Information in a Secured Area

Authorized Representatives shall keep all Protected Material or notes or memoranda related thereto in a secure, locked location with access limited to an Authorized Representative.

8. Responsibilities of Authorized Representatives

Every Authorized Representative must protect and safeguard Protective Materials at all times, shall not discuss such information with anyone who is not an Authorized Representative and shall promptly report any apparent violation of access to the company. Any Authorized Representative shall continue to be bound by this Protective Order and/or Certificate even if no longer engaged by the Commission staff or intervenor.

9. Disclosure Request

In the event staff or any party receives a notice to produce the Protected Materials or any portion thereof by way of law, regulation, directive or any other legal document, from any governmental authority or subdivision or any party in a proceeding pending before any court or administrative agency, or otherwise becomes legally compelled to disclose any of the Protected Materials, the party shall provide Company with notice of said request for Protected Materials as soon as reasonably practicable. The Company may exercise any applicable rights to oppose the disclosure of Protected Materials including, but not limited to, the seeking of a protective order, or other appropriate remedy. The party who has received such notice shall not unreasonably oppose the Company's exercise of said rights to challenge the disclosure of Protected Materials. In the event that a protective order or other remedy is not obtained, such party will furnish only that portion of the Protected Material which it is advised, by written opinion of its counsel, is legally required, and prior to the release shall advise the Company of the extent and portion of the Protected Material being produced and shall not unreasonably oppose the Company's efforts to prevent the release or public disclosure of said Protected Materials. If required by an order of a governmental or judicial body of competent jurisdiction, a party may release to such body that portion of the Protected Material which it is legally required to do and only to the extent ordered under applicable laws and stature.

10. Treatment of Information in Filings and Hearings

Staff or any party proposing to use Protected Materials on the record must notify the Company in advance and propose a specific method for preserving its confidentiality. The Company may object to such use and, if an accommodation as to the use of Protected Materials cannot be reached, the dispute shall be

presented to an Administrative Law Judge in accordance with applicable Commission rules and regulations and this agreement.

At a minimum, such method shall provide that no references to the Protected Materials shall be made in filings, briefs, motions or other pleadings, arguments, testimony or otherwise, or at any hearing, except in accordance with the Commission's rules and this Agreement. All discussion of the Protected Materials and of expenditures for security measures shall be in camera, the record thereof shall be under seal, and that portion of the public record of this proceeding shall be redacted. All public filings, insofar as related to security measures shall be redacted to remove any Protected Material and complete copies thereof shall be served only on Council of Record who are Authorized Representatives who have executed a Non-disclosure Certificate and shall be filed under seal.

Any work products or other documents developed by Staff or any party that reproduces or otherwise uses the Protected Materials will also be treated as confidential, and the same treatment will be accorded the work product or such other documents as is accorded the Protected Materials.

11. Breach of Agreement

In the event the staff, any party or Authorized Representative of the Staff or party breaches this Agreement, such person(s) and/or entity(ies) shall be responsible for damages in accordance with law and barred from presenting in this proceeding testimony, filings, briefs and arguments pertaining to expenditures for the security measures. In addition, such party shall be barred from further access to the Protected Materials.

(Usual boilerplate provisions dealing with required notices, conflict of laws, modification procedures, etc. can be added as appropriate in individual situations.)