Resolution on Guidelines for State Commission Procedures Involving the Handling of Security Sensitive Documents and the Recovery of Prudently Incurred Security-Related Costs

---

WHEREAS, State commission procedures and existing State "freedom of information" statutes governing public access to critical drinking water infrastructure information and other sensitive documents are key to limiting the likelihood of terrorist attacks involving the nation's water supplies (as well as efforts targeting critical energy or telecommunications facilities); and

WHEREAS, Current procedures and State statutes outlining the treatment of confidential information involving financial or competitive issues may not adequately address the need for differential treatment and handling of security sensitive materials; and

WHEREAS, Review of current procedures related to the treatment of security sensitive documents internally, in hearings, and in response to document requests, may be needed to determine adequacy, applicability and effectiveness of current procedures; and

WHEREAS, Jurisdictional water companies, in efforts to enhance security to meet current threats, may be incurring expenses of an extraordinary nature; and

WHEREAS, The Water Committee has attached a proposed minimum checklist of some items commissions may wish to consider when examining their policies on treatment of security sensitive information; and

WHEREAS, Additional recommendations on reforming

procedures to handle security sensitive information may be gleaned from the Federal Energy Regulatory Commission's (FERC) January 16, 2002 Notice of Inquiry into availability of critical energy infrastructure information (Docket Nos. RM02-4-000 and PL02-1-000), which suggests commissions might determine what data is critical, consider the extent to which requests can be handled outside of the State's freedom of information procedures, determine the requester's status and need for the information, verify the requester's identity and authorization to act on behalf of an organization, the role to be played by non-disclosure agreements, and consideration of any ex parte issues; and

WHEREAS, The National Association of Water Companies Rates and Revenue Committee (NAWCRRC) has also provided a discussion paper on security costs and confidentiality to the Water Committee; and

WHEREAS, The FERC also recently issued a Policy Statement regarding recovery of prudently incurred security related costs; now therefore be it

RESOLVED, That the Board of Directors of the National Association of Regulatory Utility Commissioners (NARUC) convened in special session in a March 13, 2002 teleconference call, encourages Commissions having effective procedures related to limiting public access to security sensitive information to share these procedures with Commissions embarking on the review or the enhancement of existing procedures and coordinate with the NARUC Ad Hoc Committee on Critical Infrastructure to the extent applicable; and be it

further

RESOLVED, That NARUC's member commissions are encouraged to review the appropriate treatment of all security sensitive documents accessible to the public and consider the suggestions offered in the attached Water Committee Minimum Checklist, the attached NAWCRRC recommendations, and the FERC proceedings cited earlier; and be it further

RESOLVED, That State Commissions are also encouraged to inquire what security-related steps jurisdictional utilities have taken, to coordinate with local or appropriate law enforcement agencies or with an information clearinghouse such as the State's emergency management agency, and to identify and /or establish procedures for timely recovery of prudently incurred security related costs; and be it further

RESOLVED, That the appropriate NARUC Industry Sector Committees are encouraged to monitor the ongoing security efforts of State and Federal Agencies, as well as industry actions/initiatives and continue to offer recommendations on infrastructure security as new and improved procedures are developed.

Proposed Minimum Checklist for Commission Review of Security Sensitive Information

The Water Committee has reviewed information from several sources and recommends State Commissions consider the following:

I. WEBSITE REVIEW:

State Commission's may wish to initiate a specific review of their websites to assure that it does not contain any security sensitive material that should be removed.

II. INTERNAL SECURITY/DOCUMENT REQUESTS:

States' may wish to initiate rule and statutory changes to insure procedures governing public requests for security sensitive data include one or more of the following recommendations:

- Requests for security sensitive information should be accepted only in writing and only from individuals with verified identification.
- Records management personnel should retain all requests and copies of identification for written requests and consider including, for "in-person" written requests, the use of video records, fingerprints or any other appropriate technology to maintain a more comprehensive record of the transaction.
- Any suspicious requests for security sensitive information should be referred to a designated State or Commission individual for appropriate processing.

In reviewing the effectiveness of existing procedures, State Commissions' may wish to consider:

- If existing regulations or policy for confidential treatment of private information or proprietary information may legally be extended to include information relating to security; if not, amendments to existing procedures should be made.
- If the Commission process for utility requests for limiting the availability of certain information is expeditious and streamlined.
- Once the request is approved, if the Commission's physical isolation of documents is secure in that access to Commission employees, parties of record and members of the public is appropriately limited.
- In addition to procedures related to the storage of documents deemed to have restricted public availability, procedures for maintaining confidentiality during public hearings should also be addressed.

- If security clearances should be assigned to designated employees who shall be in charge of maintaining security sensitive information and/or requiring certificates of non-disclosure to be signed by employees, parties of record or others who have access to the information.
- If security sensitive materials may be better stored at the utility than the Commission subject to commission verification that the document exist and are being kept up to date, e.g., emergency response plans, risk management plans, vulnerability assessments, engineering blueprints, distribution system maps, topographic maps, lists of hazardous chemicals, or any other critical infrastructure information.

Sponsored by the Committee on Water

Adopted by the NARUC Board of Directors March 13, 2002