

Summary of the “Drinking Water System Security Act” May 20, 2009 Draft

Requirements on community water systems serving more than 3,300 people:

- *Update and submit to EPA vulnerability assessments completed pursuant to SDWA Sec. 1433 at least every 5 years, and promptly after a major change to the water system (such as building a new treatment plant).*
- *Update emergency response plans completed pursuant to SDWA Sec. 1433, update at least every 5 years, and certify to EPA that the ERP has been completed and/or updated.*
- *Develop and submit to EPA a site security plan that addresses vulnerabilities using layered security measures, and update the plan at least every 5 years. For facilities that EPA has identified as at risk of an attack resulting in the release of a “substance of concern” (such as gaseous chlorine), the site security plan must include an assessment of “methods to reduce the consequences of a chemical release from an intentional act,” which is a review of “inherently safer technology” (IST) disinfection options. These utilities must also state whether it intends to implement one of the reviewed IST options.*
- *Submit the IST assessment (but not the entire site security plan) to the state SDWA enforcement agency, if the utility is in a state with primary SDWA enforcement authority.*
- *VAs or SSPs must describe “appropriate roles or responsibilities” that facility employees must perform to “deter or respond to” terrorist attacks.*
- *Water systems must involve certain employees in the development of VAs and SSPs, and provide at least 8 hours of annual training to relevant employees on security roles and responsibilities.*

Requirements on EPA:

- *Establish at least 4 risk-based tiers comprised of water systems based on the potential consequences of a terrorist attack at the water facility, including at least one “high-risk” tier.*
- *Work with DHS to compose a list of “substances of concern” and threshold quantities for the release or theft of each substance. The list must take into account chemicals listed in DHS’ Appendix A and the requirements of Sec. 112(r) of the Clean Air Act.*

- *Assign water systems to one of the tiers based on potential consequences of a terrorist attack on the system, including the potential for the release of a substance of concern as a result of an attack, and provide water systems with an explanation of the rationale for their risk tier assignment.*
- *Require water systems that possess a “substance of concern” at a quantity above the threshold level to review and assess IST options.*
- *Provide water systems with “baseline information” detailing the types of potential attacks that security measures should protect against.*
- *Review vulnerability assessments and site security plans submitted by utilities, and require water systems to correct “significant deficiencies” in the plans.*
- *Notify primacy states of “significant deficiencies” in IST assessments submitted by utilities and require utilities to correct the deficiencies. Primacy state would then, based upon the corrected assessment, decide whether a high-risk tier utility must implement IST.*
- *Annually report to Congress summarizing the water sector’s progress in complying with the regulations. The report may not include protected information or information about individual water facilities.*
- *Establish a grant program to train water system employees on security roles and responsibilities. This program confers no requirements on water systems.*

Requirements on SDWA Primacy State Enforcement Agencies:

- *Upon receipt of an IST assessment from a utility in a high-risk tier that has decided against implementation of IST, the primacy state must decide whether to require the utility to implement IST.*
- *If a primacy state decides to not require a utility to implement IST, the process concludes. EPA cannot review the decision or require the implementation of an IST at a utility in a primacy state after the primacy state has acted.*
- *If a primacy state decides to require a utility to implement IST, the state must consider and examine several factors, including whether the IST would reduce the impacts of the release of a “substance of concern” from a terrorist attack, whether the IST would threaten the utility’s compliance with SDWA, and whether the implementation of the IST is feasible for the utility.*
- *If a primacy state fails to make a determination of whether a high-risk utility must implement IST, and still does not make a determination after notification by EPA, then EPA may make a decision on whether the high-risk utility must implement IST.*

Information Protection Provisions:

- *Defines vulnerability assessments, site security plans, documents related to EPA's review of such assessments and plans, documents related to inspections, and other information as "protected information" that is not subject to public disclosure under the Freedom of Information Act or any state or local law.*
- *EPA is directed to produce standards for the sharing of protected information with federal, state, and local officials including first responders and law enforcement officials, water facility employees with security responsibilities, and designated employee representatives.*
- *EPA is directed to "set penalties for the unlawful sharing of protected information."*
- *In judicial proceedings in which a party seeks access to protected information, the information is treated as "Sensitive Security Information" and may only be disclosed to counsel for the party seeking access if granted by a judge. The judge would also determine the terms and conditions of access to the information. An order granting access may be appealed, and civil penalties may be imposed on attorneys that disclose protected information.*

Other Provisions:

- *Exempts drinking water systems subject to this Act from the Department of Homeland Security's CFATS regulations.*
- *This draft does not cover wastewater facilities. Under legislation being developed by the House Homeland Security Committee, wastewater facilities would be subject to CFATS.*
- *Authorizes \$190 million for the program in 2011, with \$30 million reserved for administrative costs at EPA and the remainder to help utilities comply with the Act through the update of vulnerability assessments, site security plans, and emergency response plans, the implementation of security measures, and the costs of implementing IST.*
- *Authorizes "such sums as may be necessary" for the same purposes in 2012 through 2015.*
- *Allows EPA to audit and inspect water systems to determine compliance with the security regulations.*

- *Consistent with current law, allows states to impose more stringent requirements on water systems.*
- *Directs EPA to promulgate final regulations to implement the legislation within two years.*