National Rural Water Association
Duncan, Oklahoma
www.nrwa.org

TO: National Institute of Standards and Technology (NIST)
FROM: National Rural Water Association
CONTACT: Mike Keegan, Analyst
DATE: April 8, 2013
SUBJECT: The NIST Comprehensive Review to Develop a Cybersecurity Framework

---

The National Rural Water Association has over 30,000 small and rural community members with drinking water and/or wastewater supplies. We are writing to express our eagerness to initiate a partnership with NIST (Cybersecurity Framework) to secure the country's 51,651 drinking water and 16,255 sanitation supplies from cyber attacks. Most of these water supplies serve small communities with limited public resources and competing public welfare priorities (94% of community water systems serve less than 10,000 persons and 80% of public sewer systems serve less than 10,000 persons).

By collaborating with the water sector, and utilizing the existing network that water supplies rely on for security initiatives and education, the Cybersecurity Framework could: (1) rapidly assess all of the water supplies efficacy in protecting their cyber infrastructure, (2) develop reasonable protocols to enhance protection, (3) provide assistance to any inadequate cyber protection plan, and (4) document the state of the cyber protection in all water supplies. Upon adoption/completion of a cybersecurity plan, each community will have a documented security plan that could be verified and open to review as appropriate. Federal, state and local authorities could easily track which communities have taken the initiative to secure their cyber infrastructure. The contents of each plan could be combined with each community's vulnerability assessment and emergency response plans.

In the past, similar types of security initiatives have been uniquely successful in that they expeditiously advanced measurable security initiatives in water systems with the support of the local communities. For example, for compliance with the Bioterrorism Act of 2002, the U.S. EPA found that over 90% of small community water supplies relied on the rural water cooperative approach for completing security vulnerability assessments (VA) in a matter of months – at no cost to the communities. The Bioterrorism Act's requirement for communities to adopt VAs was crafted in such a way to allow each unique community to address and prioritize their community's particular vulnerabilities. This type of local tailoring is essential in crafting the most protective security plans, because every community has unique vulnerabilities. It also has the additional benefit of promoting local support for security initiatives versus a uniform regulatory approach, which often results in local resistance, because it forces communities to dedicate limited funding and resources they see as unnecessary. The few communities who were not aware of the rural water initiative for completing the vulnerability assessments faced compliance costs over $10,000, and likely viewed the initiative as just one more unfunded federal mandate.

Local support and responsibility is essential to ensure security protection because only local experts can identify the most vulnerable elements in the community and detect immediate threats. A national collaborative Cybersecurity Framework for water supply protection initiative should result in communities enthusiastically focusing on enhancing local security based on local risks.

Thank for the opportunity to comment on the Cybersecurity Framework. We are eager to begin a partnership with NIST to advance cybersecurity protection objectives in the nation's water and sanitation supplies.

The National Rural Water Association represents over 30,000 small and rural community members, dedicated to drinking water quality, environmental protection and public health protection.