Request for Information

Federal Register / Vol. 78, No. 38 / Tuesday, February 26, 2013 / Notices

National Institute of Standards and Technology
[Docket Number 130208119–3119–01]

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Comments submitted by Dan Schmelling and Steve Allgeier, U.S. Environmental Protection Agency

Current Risk Management Practices

1. *What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?*

A significant challenge in the water sector is the absence of an industry standard. In general, water utilities will strive to operate according to industry standards of design and practice. Currently, a great deal of guidance on cybersecurity is available, but there is no commonly accepted standard of practice for water utilities. Thus, water utilities must determine for themselves what cybersecurity practices to adopt, including which cybersecurity risks justify the investment of resources to reduce. This situation is especially challenging given the significant resource constraints that utilities face.

Another challenge is the difficulty of adding security to existing industrial control systems that may have been designed with minimal security and may not support more robust security practices. Further, assessing cybersecurity risks is challenging due to a lack of information regarding threats, specific vulnerabilities, likelihood of attack, potential consequences, and the efficacy of various countermeasures or mitigation strategies. Lack of information in these areas makes it hard to define appropriate security requirements. The water sector produced a document, *Roadmap to Secure Control Systems in the Water Sector*, which discusses these and other challenges in more detail.

2. *What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?*

While there are commonalities among process control systems across sectors, there are significant disparities in the actual or perceived consequences of cyber attacks on those systems. Such consequences will influence perspectives in a sector on the appropriate level of resources to invest to reduce cyber risks (and, thus, appropriate standards of practice).

There are also significant disparities across sectors in the resources and technical skills available to implement an effective cybersecurity strategy. In the water sector, for example, the expenditure of resources to make control systems more secure against cyber attacks must be balanced against major unfunded infrastructure replacement needs.

3. *Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?*

The water sector was subject to the Bioterrorism Act of 2002, which required community drinking water systems serving more than 3,300 people to conduct vulnerability assessments (http://water.epa.gov/infrastructure/watersecurity/lawsregs/bioterrorismact.cfm). EPA developed guidance for the sector regarding the threats to consider when performing these assessments, which can be found in *Baseline Threat Information for Vulnerability Assessments of Community Water Systems*. This guidance encouraged utilities to consider physical, contamination, and cyber threats, as well as interdependencies among critical infrastructure sectors.

EPA recommends that water utilities manage risk by updating regularly (e.g., every five years or after a major process change) an all-hazards vulnerability assessment. Cyber attacks are a type of threat that should be included in this assessment. The results of the vulnerability assessment should allow resources to be prioritized to reduce the most significant risks. EPA provides tools such as the Vulnerability Self Assessment Tool (VSAT) that utilities may use to conduct these vulnerability assessments.

5. *How do organizations define and assess risk generally and cybersecurity risk specifically?*

The water sector uses the DHS definition of risk as the product of threat*vulnerability*consequence. Water sector risk assessment tools, such as VSAT noted above, assess risk by analyzing each threat paired with each applicable asset. Cybersecurity risks should be assessed as a type of threat in this process.

7. *What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?*

The water sector has a risk assessment standard, *J100 RAMCAP Standard for Risk and Resilience Management of Water and Wastewater Systems*. This standard includes cyber attacks as a potential threat (insider and outsider cyber attacks for process sabotage, diversion, or theft). A number of risk assessment tools are being developed or enhanced to comply with this standard. In addition, water utilities may use additional tools for specific risk areas, such as CSET or CS2SAT for assessing cyber risks.

8. *What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?*

Cybersecurity in the water sector is not regulated, and there are no reporting requirements associated with it.

9. *What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?*

The water sector has significant interdependencies with other sectors. Specifically, the water sector is dependent upon the energy, transportation, communications, and chemical sectors. Furthermore, the following sectors are dependent on the water sector for their operations: critical manufacturing, energy, food and agriculture, and healthcare and public health.

12. *What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?*

As noted under question 1, a significant challenge to improving cybersecurity practices across the water sector is the absence of a standard of practice. The development of a national standard for cybersecurity in the water sector would set an important goal that water utilities would strive to meet.

Use of Frameworks, Standards, Guidelines, and Best Practices

7. *When using an existing framework, should there be a related sector-specific standards development process or voluntary program?*

Yes. Due to disparities in risks, challenges, and resources to implement cybersecurity across sectors, there should be sector-specific standards. In addition, a sector-specific voluntary program could significantly increase the degree to which a sector adopts a cyber security standard. Such a program should focus on awareness, risks, benefits, and training on implementation.

8. *What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?*

Sector coordinating councils, including the sector-specific agency, should play a lead role both in developing a sector-specific cyber security standard and carrying out a voluntary program to promote the use of it. In the water sector, for example, the sector coordinating council has already assessed risks, challenges, potential solutions, and goals related to cyber security in the document *Roadmap to Secure Control Systems in the Water Sector*. This effort puts the sector coordinating council in a knowledgeable position to adapt a general standard into specific guidelines that will meet the needs of the sector. Further, members of the sector coordinating council have the contacts and credibility to promote effectively the use of a cybersecurity standard within a sector.

Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

1. *Separation of business from operational systems;*
2. *Use of encryption and key management;*
3. *Identification and authorization of users accessing systems;*
4. *Asset identification and management;*
5. *Monitoring and incident detection tools and capabilities;*
6. *Incident handling policies and procedures;*
7. *Mission/system resiliency practices;*
8. *Security engineering practices;*
9. *Privacy and civil liberties protection.*

In the water sector, practices 1 through 4 have been generally applied to the industrial control systems used in treatment, operation, and distribution. However, there is a growing trend to collect more information in control systems and make that information more easily accessible. For example, a SCADA may exist on a network separate from the business network, but data from remote monitoring or control sites may be transmitted back to SCADA over a wireless network. Utilities following best practices would use encryption and firewalls to protect the SCADA, but this may be insufficient to protect against certain cyber threats.

In the water sector, practice 6 has been adopted to some extent by most utilities, but in a general sense not specifically related to cyber security. Specifically, most water utilities serving more than 3,300 people have developed emergency response plans that guide a utility's response to a range of incidents (i.e. all hazards response planning). It is possible that a well developed emergency response plan could help a utility effectively respond to the physical consequences of a cyber attack intended to sabotage a critical asset.