Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on Water Security Practices, Incentives, and Measures

June 2005

FOREWORD

This report presents the U.S. Environmental Protection Agency's Administrator the recommendations of the National Drinking Water Advisory Council (NDWAC) on water security practices, incentives, and measures.

A draft report was prepared by the NDWAC's Water Security Working Group (WSWG). The WSWG was composed of a diverse set of interests and perspectives on water security, including representatives of public and private and large and small water and wastewater utilities, public health agencies and advocates, environmental regulators, rate setters, and public interest groups. The charge from the Council to the WSWG was to develop findings that address security practices, incentives for improvements in security, and measures of security progress. In response to this charge, the WSWG reached consensus on 18 findings that: 1) establish the features of active and effective security programs, 2) identify ways government and others might encourage utilities to adopt and maintain active and effective programs, and 3) suggest utility-specific and national measures of water sector security progress.

The WSWG presented their findings to the NDWAC in June 2005. After discussion and deliberation, the Council unanimously approved and adopted the WSWG's findings unchanged, and elevated these findings to the status of recommendations to the Agency.

TABLE OF CONTENTS

Abstract
Executive Summary i
Set minimum expectations for security program outcomes, with substantial flexibility for design of utility-specific implementation approaches and tactics ii
Keep security programs fresh and up-to-date, and emphasize inherently more secure practices iv
Create awareness and support for water security iv
Invest in water security v
Form strong, durable partnerships v
Findings in Sequential Order vii
Security vii
Incentives ix
Measures x
I. Introduction 1
Charter and Mission of the Working Group 2
Working Group Composition 2
Security-Sensitive Information 3
The Deliberative Process and Consensus 3
Scope and Application of WSWG Findings 4
II. Security 7
Approach to Developing Findings on Security 7
Summary of Findings on Security 8
One Size Does Not Fit All 8
Security Program Scope 9
Significant System Failures and Key Threats 11
Principles That Support Active and Effective Security Programs 12
Security Program Features 13
Ongoing Improvement 15
Improve Connections with Public Health 16
Support Development of Contaminant Monitoring Technologies 16
III. Incentives 17
Approach to Developing Findings on Incentives 17
Summary of Findings on Incentives 18
Understanding the Consequences of Failing to Address Security 18
Recognition 19
Peer Assistance and Review 20
Technical Assistance 20
Access to Security-Related Support and Planning 22
Financial Support 23
Rate-Setting Organizations 23
Regulation 24
IV. Measures 25
Approach to Developing Findings on Measures 25
Attributes of Sound Measures 26
Types of Measures Considered 26

Summary of Findings on Measures 27
Minimum Measures Utilities Should Use 27
Measures for Utilities to Consider 28
National Aggregate Measures 29
Other Measures Considered 34
Reporting 34

Appendix A Features and Measures of an Active and Effective Security Program
Appendix B Chart Showing Features of an Active and Effective Security Program and Corresponding Measures that Utilities Should Use
Appendix C Measures Utilities Should Consider
Appendix D Individual Comments of WSWG Members

Attachment 1 Roster of WSWG Members, Federal Resource Personnel, and Outside Experts
Attachment 2 WSWG Operating Procedures
Attachment 3 Transmittal Memo
Attachment 4 Annotated Bibliography of Security References
Attachment 5 Acronym List

ABSTRACT

The Water Security Working Group (WSWG) was charged by the National Drinking Water Advisory Council (NDWAC) with developing findings on security practices, incentives, and measures. The 16 members of the WSWG include representatives of small, medium, and large water and wastewater utilities, public health advocates and regulators, and environmental and public health interest organizations. The findings contained in the WSWG document reflect a consensus of these diverse perspectives.

The WSWG presents 18 consensus findings. Findings 1 through 6 establish a consistent expectation for what constitutes an "active and effective" water sector security program and identify 14 features that all active and effective security programs should share. These findings create a balance between providing the water sector with a more consistent basis for moving forward with security enhancements and avoiding in any way prescribing the specific security countermeasures individual utilities should use. In the realm of security, "one size does not fit all." Findings 7 and 8 address forging closer partnerships between the utility and public health communities and development of practical, affordable contamination surveillance and monitoring technologies.

Findings 9 through 15 call on EPA, DHS, state agencies, utility trade associations, and others to create incentives for development and maintenance of security programs, including: educational efforts to raise utility awareness about both the benefits of security enhancements and the potential liability resulting from a failure to address security, and to ensure that organizations which influence utility costs and revenues (e.g., rate and fee setting organizations) understand security imperatives; targeted technical assistance; creation of programs for utility peer-to-peer assistance and review; and support for inclusion of water utilities in security-related planning and exercises. They also appeal to Congress, EPA, DHS, and other federal agencies to increase grant and loan funding specifically focused on water sector security.

Findings 16 and 17 address measurement of individual security program progress. They identify "core" measures for use by all utilities during annual self assessments of security progress, and provide an additional suite of measures for utilities to consider.

Finding 18 proposes three areas of sector-wide, national aggregate measurement: (1) implementing "active and effective" security programs as measured by the degree of implementation of the 14 features of active and effective security programs; (2) reducing security risks measured by the total number of assets determined to be a high security risk and the number of former high security risk assets lowered to medium or low risk, based on the results of vulnerability assessments; and (3) reducing the inherent risk potential of utility operations measured by Clean Air Act Section 112(r) reporting on hazardous substances and by the number of utilities that convert from use of gaseous chlorine to other forms of chlorine or other treatment methods. The Group encourages EPA to work with the water sector and stakeholders to explore options for enhancing the consistency and credibility of national measurement through peer review, third party verification, blind surveys, or other more independent assessments. To address concerns about the inappropriate release of individual utility security-sensitive information, the WSWG encourages EPA to publish national measures on a strictly aggregated basis and ensure appropriate confidentiality for submitted data.

EXECUTIVE SUMMARY

Nationwide, there are over 160,000 public water systems. Together, these systems provide drinking water to over 300 million people. Public and private wastewater treatment systems serve approximately 75 percent of the U.S. population. Drinking water and wastewater systems are critical to the security of the United States because they deliver needed drinking water supplies and wastewater collection and treatment services and support the many vital services, such as fire suppression, that rely on a stable supply of water. An attack or even a credible threat of an attack on water infrastructure could seriously jeopardize the public health and economic vitality of a community.

In fall 2003, the National Drinking Water Advisory Council (NDWAC) chartered the Water Security Working Group (WSWG or "the Group") to develop findings on security practices and programs, incentives for broad adoption of security practices in the water sector, and measures to gauge the extent of implementation of security practices. The Group was comprised of 16 members representing a broad range of perspectives related to water sector security, including participants from large and small drinking water and wastewater treatment providers, rate setting organizations, technical assistance providers, the public health community at the state and local level, academia, and community interest groups. The WSWG was supported by a number of resource personnel from federal agencies with interest and expertise in water security. These included representatives from the U.S. Environmental Protection Agency (EPA), Department of Homeland Security (DHS), Department of Defense (DoD), and the Centers for Disease Control and Prevention (CDC). The WSWG also was supported by outside experts, including an expert in emergency preparedness and response nominated by the National Emergency Management Association.

The WSWG met seven times in person and by conference call between July 2004 and April 2005. Notices of meetings were published in the Federal Register in advance of meetings and calls. Except when security-sensitive information was discussed, meetings were open to the public, and opportunities for public comment were provided at each meeting. The Group found that, in general, they could accomplish their deliberations without discussion of security-sensitive information, and had only two closed sessions throughout the duration of their deliberations. They used a consensus-based, collaborative problem-solving approach to develop findings. In the few instances where the Group did not reach consensus, the range of views of the Group with respect to that issue is described.

The WSWG makes 18 findings dealing with security practices and programs, incentives, and measures. Findings address the basic scope and principles for active and effective security programs, establish significant system failures and key threats that security programs should consider, identify 14 features that all active and effective security programs should address, advise steps that government and others can take to support and encourage utility security efforts and create a better climate for security, and describe a framework for measuring utility security progress. Because the WSWG is made up of many stakeholders from different perspectives, these findings are endorsed by a wide range of interested parties, including small and large utilities, public health advocates and regulators, first responders, and environmental and public health interest organizations.

Five themes cut across the WSWG's findings and serve as the organizing structure for this executive summary. Readers are encouraged to go beyond the executive summary to the discussion of each finding in the full document to understand the depth and context of the WSWG's deliberations and findings.

Set minimum expectations for security program outcomes, with substantial flexibility for design of utility-specific implementation approaches and tactics

Finding 1 establishes the expectation of consistent security outcomes, with significant flexibility to tailor security approaches and tactics to utility-specific circumstances and operating conditions. *Finding 2* addresses the scope of active and effective security programs, and emphasizes the need for programs to address protection of public health, safety, and confidence. *Finding 3* describes the potential significant system failures and key threats that utilities should consider when developing active and effective security programs, and *Finding 4* lists principles utilities should use as they develop their utility-specific active and effective security programs.

The centerpiece of the WSWG's findings is identification of 14 features that all active and effective security programs should address, and a corresponding set of suggested program measures. *Finding 5* establishes the 14 features of active and effective security programs, each of which are described in detail in Appendix A. The text box at the right summarizes the features of active and effective security programs. *Finding 16* identifies measures that correspond to the program features. The Group expects these measures to be used by all utilities to form the basis for utility-specific security self-assessment and measurement programs. *Finding 17* encourages utilities to consider a list of additional measures that could be used to round out security measurement programs.

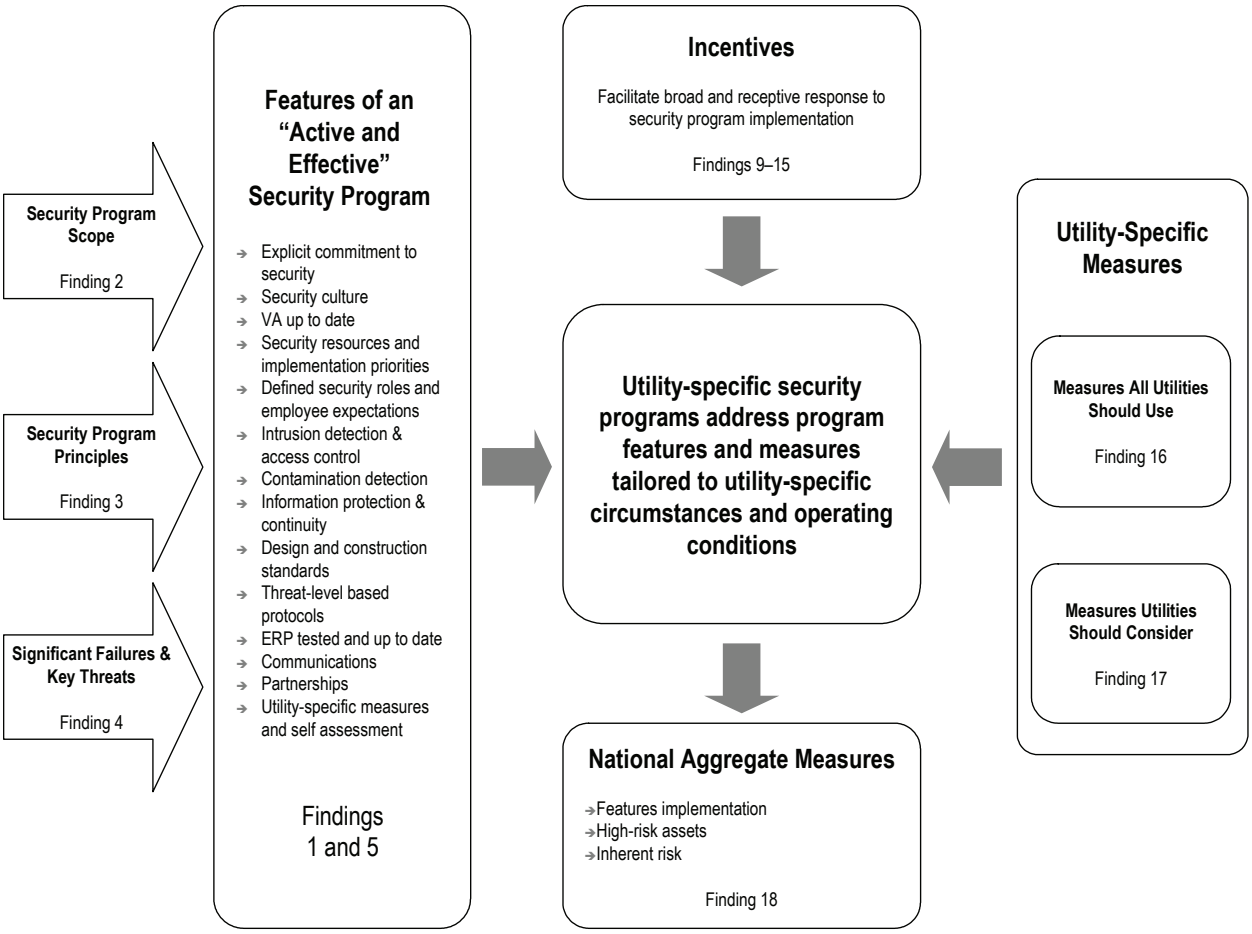
Features of an Active and Effective Security Program

1. Make an explicit and visible commitment of the senior leadership to security.
2. Promote security awareness throughout the organization.
3. Assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.
4. Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.
5. Identify managers and employees who are responsible for security and establish security expectations for all staff.
6. Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.
7. Employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.
8. Define security-sensitive information, establish physical and procedural controls to restrict access to security-sensitive information as appropriate, detect unauthorized access, and ensure information and communications systems will function during emergency response and recovery.
9. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower risk design and technology options.
10. Monitor available threat-level information; escalate security procedures in response to relevant threats.
11. Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans as necessary to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.
12. Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, and customers.
13. Forge reliable and collaborative partnerships with communities, managers of critical interdependent infrastructure, and response organizations.
14. Develop utility-specific measures of security activities and achievements, and self assess against these measures to understand and document program progress.

As a complement to the identification of consistent security program outcomes through descriptions of security program scope, principles, features, and measures, the WSWG also emphasizes the need for significant flexibility to tailor security approaches and tactics to utility-specific circumstances and operating conditions, such as size, location, water source, technology, budget, political support, and legal constraints. These and other

utility-specific circumstances and operating conditions must inform development of specific security tactics. A rigid approach that requires a certain type of fence or other access control, or a prescribed information technology protection system or a standard set of personnel security policies would, automatically, over-address security needs for some utilities and under-address security needs for other utilities.

The WSWG sees findings on security program scope, significant threats and major consequences, principles, and features coming together to inform individual utilities' development of utility-specific security approaches and tactics. That is, in developing security programs specifically tailored to their circumstances and operating conditions, utilities will address each program feature in light of the program scope, significant threats and major consequences, and principles described by the WSWG. In later findings on measures, the WSWG has equipped utilities to consistently measure their individual progress and support the emergence of national aggregate measures of sector-wide progress. Incentives encourage security progress by creating a climate that is friendly to utility security efforts. The figure below illustrates these relationships.



Keep security programs fresh and up-to-date, and emphasize inherently more secure practices

Security programs will change over time. The features and measures of active and effective security programs identified by the WSWG in *Findings 5 and 16* emphasize the importance of keeping assessments of vulnerabilities and emergency response plans up-to-date as "living" documents. They also stress the need for ongoing attention to security in annual planning and budgeting, and the need to update utility-specific security approaches and tactics to incorporate lessons learned from tabletop and field exercises, and from any actual responses. Security program features and measures also emphasize the need for utilities to take advantage of opportunities to improve security through use of plant design and operating choices that are inherently more secure or that lower the likelihood or potential consequences of a successful attack. Application of inherently safer designs and operating procedures during plant construction, upgrades, and major maintenance activities may be the most efficient way for utilities to, over time, improve security. Finally, the security program features and measures stress that, as technological and other advances give utilities opportunities to improve security they should be seized. *Finding 6* addresses this need directly, by calling on utilities to use a continual improvement approach to learn from implementation of security programs and to enhance security over time.

Create awareness and support for water security

In some ways, the water and wastewater utility industry is the silent critical infrastructure. In many communities, even after the terrorist attacks of September 11, 2001, there may be little awareness of the need to protect critical water and wastewater assets. The WSWG strongly believes that utilities need help creating awareness of the importance of water security, both within the industry and in the communities they serve. Utilities, especially small systems with limited resources, also need a support system to help identify and implement practical, cost-effective security programs.

Finding 9 calls on EPA, DHS, state agencies, and water and wastewater utility organizations to provide information on the importance of active and effective security programs to utilities, and to make utilities more aware of the benefits of active and effective security programs and the potential negative consequences of failing to address security. *Finding 10* addresses recognition of security programs. *Finding 11* calls on EPA and others to build on existing successful peer review and assistance programs, such as the Rural Community Assistance Partnership program and the Georgia/National Rural Water Association Small System Peer Assistance Team, to establish a peer assistance and review system for utility security. Advice from a trusted peer will often be the most practical, affordable, and relevant way to deliver much needed help and support for security efforts, especially in small systems. *Findings 12 and 13* address the need for technical assistance, including technology verification programs to support security efforts and the need to facilitate utilities' access to security-related support systems and infrastructure, and participation in tabletop and field exercises.

Finding 18 addresses awareness and support for security in a slightly different way, by suggesting three potential national aggregate measures of security progress:

- Implementation of "active and effective" security programs as measured by the degree of implementation of the 14 program features and corresponding feature-specific measures suggested by the WSWG;
- Reduction in security risks as measured by the total number of assets determined to be a high security risk and the number of former high security risk assets lowered to medium or low risk, based on the results of vulnerability assessments; and

› Reduction in the inherent risk potential of utility operations as measured by Clean Air Act Section 112(r) reporting on hazardous substances and by the number of utilities that convert from use of gaseous chlorine to other forms of chlorine or other treatment methods.

The three potential national aggregate measures identified by the WSWG would be presented on an aggregate basis only (i.e., individual facility results would not be available).

Invest in water security

Security will not improve without investment of time, attention, and money on the part of all partners. *Finding 8* calls on government to support and facilitate development and distribution of reliable, affordable contaminant monitoring technologies. This is critical to improve the security of distribution systems and to enable the water sector to develop effective monitoring and surveillance strategies that include more than reliance on monitoring of public health anomalies to identify potential water contamination. *Finding 14* calls for additional, direct financial support of utility security efforts, and *Finding 15* stresses the importance of education and information for utility oversight boards and rate-setting agencies so reasonable costs of utility security can be included in utility rates in a timely way.

Form strong, durable partnerships

Finally, throughout their deliberations, the WSWG returned to the need to support security with strong, durable partnerships. Utilities will not, and should not, accomplish security alone. They must work within the larger security and response communities and with their customers to improve security. The features and measures of active and effective security programs identified by the WSWG in *Findings 5 and 16* describe the importance of utilities forging connections with local law enforcement, first responders, the public health community, and with the communities and consumers they serve. In particular, the WSWG emphasizes the importance of partnerships with communities in enhancing public confidence in utilities, improving the effectiveness of security by relying on communities to notice and report suspicious events, and increasing public support for utility security efforts. The WSWG was also particularly interested in improving partnerships between utilities and the public health community. *Finding 7* addresses this interest specifically by calling for stronger relationships between water and wastewater utilities and the public health community.

FINDINGS IN SEQUENTIAL ORDER

Security

Finding 1: Water and wastewater utility security programs should achieve consistent outcomes using utility-specific tactics and implementation approaches that are tailored to individual utilities' circumstances and operating conditions.

Finding 2: Active and effective security programs should address protection of public health, public safety (including infrastructure), and public confidence.

Finding 3: Active and effective security programs should consider six significant system failures and four key threats, as described below.

Significant System Failures

1. Loss of pressurized water for a significant part of the system.
2. Long-term loss of water supply, treatment, or distribution.
3. Catastrophic release or theft of on-site hazardous chemicals affecting public health.
4. Adverse impacts to public health or confidence resulting from a contamination threat or incident.
5. Long-term loss of wastewater treatment or collection capacity.
6. Use of the collection system as a means of attack on other targets.

Key Threats

1. Physical disruption of core facilities, such as chemical storage, or interdependent infrastructure, such as power and transportation, either through direct physical targeting or as a result of collateral damage.
2. Chemical, biological, or radiological material used to contaminate water supplies or infrastructure.
3. Cyber attack on information technology assets to disrupt service and/or obtain confidential information.
4. Use of conveyance tunnels or storm, sanitary, or combined sewers to stage an attack against utilities or other targets.

Finding 4: Active and effective security programs should be built around 11 principles, as described below.

1. Security should be part of organizational culture and the day-to-day thinking of front-line employees, emergency responders, and management.
2. A strong commitment to security by organization leadership and by the supervising body, such as the utility board or rate-setting organization, is critical to success.
3. There is always something that can be done to improve security. Even when resources are limited, the simple act of increasing organizational attentiveness to security will reduce threat potential and increase responsiveness. Preparedness itself can help deter attacks.
4. Prevention is a key aspect of enhancing security.
5. Movement towards practices that are inherently safer (i.e., have a lower risk potential) may enhance security.

6. Security programs require ongoing management and monitoring, and an ongoing budget commitment. A continual reassessment model, where changes are implemented over time as experience with security increases, may be useful.
7. Consideration of security issues should begin as early as possible in facility construction (i.e., it should be a factor in building plans and designs).
8. The relationship between practices that increase safety and those that increase security must be recognized and managed. Safety and security may complement each other, may be neutral, or may conflict. For example, a supervisory control and data acquisition (SCADA) system provides valuable operating safety information, but may also introduce a vulnerability that someone could use to cause harm or mislead operators. Similarly, permanently locking a door for security reasons might create a safety barrier to an emergency exit.
9. Strong relationships with response partners and the public strengthen security and public confidence.
10. Investment in security should be reasonable considering utilities' specific circumstances. Where threat potential or potential consequences are greater, greater investment is likely warranted.
11. Develop security programs in a way that helps communities understand the need for a security program and the utility's overall security management approach, consistent with the need to hold security sensitive information (i.e., attributable information about utility-specific vulnerabilities and security tactics) closely.

Finding 5: Active and effective security programs should include 14 features, described below.

1. Make an explicit and visible commitment of the senior leadership to security.
2. Promote security awareness throughout the organization.
3. Assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.
4. Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.
5. Identify managers and employees who are responsible for security and establish security expectations for all staff.
6. Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.
7. Employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.
8. Define security-sensitive information, establish physical and procedural controls to restrict access to security-sensitive information as appropriate, detect unauthorized access, and ensure information and communications systems will function during emergency response and recovery.
9. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower-risk design and technology options.
10. Monitor available threat-level information; escalate security procedures in response to relevant threats.
11. Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans as necessary to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.
12. Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, and customers.
13. Forge reliable and collaborative partnerships with the communities, managers of critical interdependent infrastructure, and response organizations.

14. Develop utility-specific measures of security activities and achievements, and self assess against these measures to understand and document program progress.

Finding 6: Water and wastewater utilities should reassess and seek to improve their security programs on an ongoing basis.

Finding 7: Relationships between the water and wastewater utility sector and the public health sector should be strengthened.

Finding 8: Development and distribution of reliable, affordable contaminant monitoring technologies is important to improving utility security and should be facilitated and supported by government.

Incentives

Finding 9: EPA, DHS, state agencies, and water and wastewater utility organizations should provide information on the importance of active and effective security programs to utilities and should make owners and operators more aware of the benefits of active and effective security programs and of the potential negative consequences of failing to address security.

Finding 10: EPA, DHS, state agencies, and water and wastewater utility organizations should develop programs and/or awards that recognize utilities that develop and maintain active and effective security programs, and that demonstrate superior security performance.

Finding 11: EPA, DHS, state agencies, and water and wastewater utility organizations should support development and implementation of a voluntary utility security peer technical assistance and review program.

Finding 12: EPA, DHS, state agencies, and water and wastewater utility organizations should help utilities develop active and effective security programs by providing different types of technical assistance, including technology verification information.

Finding 13: EPA, DHS, and other federal and state agencies should support utility security programs by helping utilities obtain access to needed security-related support systems and infrastructure, and by supporting inclusion of utilities in security exercises.

Finding 14: Congress, EPA, DHS and other federal agencies should support security enhancements with grant and loan programs focused on security.

Finding 15: Utility governing bodies should recognize costs associated with implementing active and effective security programs. EPA, DHS, state agencies, and utility organizations should provide educational and other materials to boards and rate setting organizations to help them understand security costs.

Measures

Finding 16: At a minimum, utility self assessment and measurement should include 13 measures, described below.

1. Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?
2. Are incidents reported in a timely way, and are lessons learned from incident responses reviewed, and as appropriate, incorporated into future utility security efforts?
3. Are reassessments of vulnerabilities made after incidents, and are lessons learned and other relevant information incorporated into security practices?
4. Are security priorities clearly identified, and to what extent do security priorities have resources assigned to them?
5. Are managers and employees who are responsible for security identified?
6. To what extent are methods to control access to sensitive assets in place?
7. Is there a protocol/procedure in place to identify and respond to suspected contamination events?
8. Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how do control measures perform under testing?
9. Is there a protocol/procedure for incorporation of security considerations into internal utility design and construction standards for new facilities/infrastructure and major maintenance projects?
10. Is there a protocol/procedure for responses to threat level changes?
11. Do exercises address the full range of threats—physical, cyber, and contamination— and is there a protocol/procedure to incorporate lessons learned from exercises and actual responses into updates to emergency response and recovery plans?
12. Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns, and is there an up-to-date list and protocol for contacting emergency response partners?
13. Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, and response organizations been established?

Finding 17: In developing their self-assessment and measurement programs, water and wastewater utilities should consider the security program measures listed in Appendix C.

Finding 18: EPA should consider three potential measures of national, sector-wide, aggregate progress described below.

1. Implementation of "active and effective" security programs as measured by the degree of implementation of the 14 program features and corresponding feature-specific measures suggested by the WSWG.
2. Reduction in security risks as measured by the total number of assets determined to be a high security risk and the number of former high security risk assets lowered to medium or low risk, based on the results of vulnerability assessments.
3. Reduction in the inherent risk potential of utility operations as measured by Clean Air Act Section 112(r) reporting on hazardous substances and by the number of utilities that convert from use of gaseous chlorine to other forms of chlorine or other treatment methods.

I. INTRODUCTION

Nationwide, there are over 160,000 public and private water systems. Together, these systems provide drinking water to over 300 million people. Wastewater treatment systems serve approximately 75 percent of the U.S. population. These systems are critical to the security of the United States not only because they deliver needed drinking water supplies and wastewater collection and treatment services, but also because they support the many vital services, such as fire suppression, that rely on a stable supply of water. An attack, or even a credible threat of an attack, on water infrastructure could seriously jeopardize the public health and economic vitality of a community.

As with other critical infrastructure sectors, concern over security at water utilities increased dramatically after the September 11, 2001 terrorist attacks on the World Trade Center and the Pentagon. Immediately after the attacks, the U.S. Environmental Protection Agency (EPA) and the drinking water and wastewater industries launched a number of initiatives to develop training and guidelines on water security. As part of this effort, initial support was provided for development of methodologies and training for community water systems on assessment of water system vulnerabilities and development of emergency response plans. Ongoing efforts to create the Water Information Sharing and Analysis Center (WaterISAC), a secure system used to disseminate security alerts and allow water and wastewater utilities to exchange ideas about security related issues, were accelerated. In June 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act (Bioterrorism Act). Among other things, the Bioterrorism Act requires each community water system that serves more than 3,300 individuals 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." The Bioterrorism Act also requires preparation—or where necessary, revision—of "an emergency response plan that incorporates the results of vulnerability assessments."

Investment in water security efforts, both public and private, also increased after September 11, 2001. In fiscal year 2002, EPA awarded approximately $51 million in grants to help the largest community water systems—those serving populations greater than 100,000—to complete vulnerability assessments. Since 2002, EPA has provided over $150 million in support for development of water security related tools, training, and technical assistance to the water sector, states, and other supporting partners.

As of the writing of this document, 100 percent of large and medium utilities and 93 percent of small community water systems covered by the Bioterrorism Act have completed vulnerability assessments, and 100 percent of large systems, 94 percent of medium systems, and 79 percent of small systems have completed emergency response plans. While this represents real progress, much work remains to be done. Understanding vulnerability is only the first step in improving security. Many water systems that have completed vulnerability assessments are now considering what steps to take to address their vulnerabilities. In the proliferation of security-related guidelines, products, services, and consultants that have appeared since September 11, 2001, water utilities are faced with a complex set of decisions about how best to invest what will inevitably be limited security funding. In this context, the National Drinking Water Advisory Council (NDWAC), in consultation with EPA, chartered the Water Security Working Group (WSWG or "the Group") to provide a forum for the many diverse security-related interests to provide much needed guidance for NDWAC and EPA security-related efforts.

Charter and Mission of the Working Group

The WSWG was established and charged by the NDWAC, an independent federal advisory council under the Federal Advisory Committee Act. The NDWAC advises, consults with, and makes findings related to EPA's activities, function, and policies under the Safe Drinking Water Act. From time to time, the NDWAC forms working groups to deliberate on a specific area of interest and to report back to the Council. The WSWG is one such group. The NDWAC directed the WSWG to:

- Identify, compile, and characterize best security practices and policies for drinking water and wastewater utilities, and provide an approach for considering and adopting these practices and policies at a utility level;
- Consider mechanisms to provide recognition and incentives that facilitate a broad and receptive response among the water sector to implement these best security practices and policies, and make findings as appropriate; and
- Consider mechanisms to measure the extent of implementation of these best security practices and policies, identify the impediments to their implementation, and make findings as appropriate.

Early in their deliberations, the WSWG rejected use of the term "best" to describe their work on security practices. The Group was concerned that defining "best" security practices would seem too much like a prescription of specific activities across the water and wastewater sector. Given the variety of utility-specific circumstances and operating conditions that exist in the water and wastewater sector, the WSWG rejected the notion that such a prescription could be developed, or if developed, fulfilled. Instead, the Group chose to make findings identifying and describing the scope, principles, and features of "active and effective" security programs, and to make related findings on improving the climate for water and wastewater security. Otherwise, the Group did not amend or modify its charge from the NDWAC.

Working Group Composition

The WSWG was made up of 16 members representing a broad range of water security perspectives. WSWG membership included participants from: large and small drinking water and wastewater treatment providers, rate setting organizations, technical assistance providers, the public health community at the state and local level, academia, and environmental interest groups. Group members were selected by EPA from among more than 80 nominated individuals. Selections were made considering the expertise and experience needed to provide advice on best security practices, incentives, and measures, and the desire to provide balanced representation across the water sector. To facilitate communication between the NDWAC and the WSWG, three members of the NDWAC were appointed to the WSWG. Because the WSWG is made up of many stakeholders from different perspectives, these findings are endorsed by a wide range of interested parties, including small and large utilities, public health advocates and regulators, first responders, and environmental and public health interest organizations.

The WSWG was supported by a number of resource personnel from federal agencies with interest and expertise in water security. These included representatives from EPA, the Department of Homeland Security (DHS), the Department of Defense (DoD), and the Centers for Disease Control and Prevention (CDC). The WSWG also was supported by outside experts, including an expert in emergency preparedness and response nominated by the National Emergency Management Association. Federal resource personnel and outside experts participated in WSWG deliberations by providing background, context, or other information or expert opinion, as called

upon to do so by a member of the WSWG or the facilitation team. Federal resource personnel and outside experts did not participate in WSWG decision making.

A roster of WSWG members, federal resource personnel, and outside experts is provided as Attachment 1.

Security-Sensitive Information

The WSWG established special procedures for deliberations on security-sensitive information. For purposes of their deliberations, the WSWG agreed that security-sensitive information would be identified as:

- Information on system-specific, attributable tactical security procedures; or
- Integrated or aggregated detail on security (e.g., by aggregating information from previously un-aggregated sources) that creates a clear picture of a specific targeting or attack opportunity.

Information already available in the public domain in the same form and at the same level of detail as discussed by the WSWG was not considered security sensitive.

WSWG meetings were closed to the public as necessary to provide a forum for WSWG members to discuss security-sensitive information. Protocols for closure of WSWG meetings to the public and discussion of security-sensitive information are included in Attachment 2, WSWG Operating Procedures. The WSWG agreed that, to maximize the usability of their document, they would strive to limit inclusion of security-sensitive information in the written materials they consider and produce. In practice, the WSWG found that closing deliberations to the public generally was not necessary, and that open meetings did not prevent substantive deliberations on the features and measures of active and effective security programs. In the few instances where the WSWG needed to discuss specific, attributable security tactics or examples, they used closed sessions. Over the course of approximately 92 hours of deliberations, the WSWG conducted only approximately 11 hours in closed session.

The Deliberative Process and Consensus

The WSWG met in person five times between July 2004 and April 2005, and had two full Group conference calls during that period. Notices of Group meetings and full Group conference calls were published in the Federal Register. Except where security-sensitive information was discussed, meetings were open to the public. Opportunities for public comment were provided at each meeting. Agendas and summaries of WSWG meetings are available on the EPA NDWAC website at www.epa.gov/ogwdwndwac/council.html.

The WSWG used a consensus-based, collaborative problem-solving approach to developing findings. In cases where the Group did not reach consensus, the range of views of the Group are described. At the end of the consensus-based process, WSWG members also had an opportunity to submit up to three pages of individual comments. Two WSWG members chose to submit Individual comments, which can be found in Appendix D.

The WSWG was served by two co-chairs. To facilitate communication with the NDWAC, one of the WSWG co-chairs was also a member of NDWAC. This individual was identified by EPA and the facilitation team in consultation with the three NDWAC members who serve on the WSWG. The second co-chair was identified by the Group using a weight of preferences selection process.

The role of the WSWG co-chairs was to act as a sounding board for the facilitation team between WSWG meetings, open and close the WSWG meetings, assist the facilitation team in running the meetings, and approve WSWG meeting summaries. The co-chairs also participated in deliberations and decision making as full members of the WSWG. The co-chairs did not determine the WSWG agenda or findings any more or less than other WSWG members.

Additional detail on the WSWG process is available in Attachment 2, WSWG Operating Procedures.

Scope and Application of WSWG Findings

The WSWG findings address all three parts of the charge given to the Group by the NDWAC: security practices or programs; incentives; and measures. The WSWG developed findings to apply to all water and wastewater utilities, irrespective of size, location, ownership, or regulatory status. The Group recognizes that the Bioterrorism Act requirements for water security apply only to community water systems that serve more than 3,300 people; however, it does not intend to limit its findings to such systems. While the Bioterrorism Act encompasses approximately 91 percent of the population served by drinking water systems, it addresses only 16 percent of systems. The vast majority of systems serve populations of 3,300 or fewer.

The WSWG decided not to limit its findings to community water systems that serve 3,300 or more people for three reasons. First, the Group believes that all utilities, regardless of type and size, need to take steps to address security. Although threats may be greater or lesser depending on utility-specific circumstances and operating conditions, no utility is immune from attack. Second, the 14 elements of an active and effective security program contain considerable flexibility to allow for utility-specific security tactics and approaches. This encourages utilities to tailor security programs to the level of resources they can devote to security and to nest security efforts in broader utility operations designed to safeguard water quality and utility infrastructure. The WSWG believes that the steps needed to address the features of an active and effective security program are, in many cases, consistent with the steps needed to maintain technical, management, and operational performance capacity related to overall water quality, and that many small utilities may be able to craft active and effective security programs with minimal, if any, capital investment.

Third, the WSWG's findings on active and effective security programs create voluntary guidelines. While the Group encourages all utilities to consider these findings and to develop active and effective security programs, there are currently no federal regulations on water security, and the Group as a whole is not suggesting federal regulations. Without regulations, it is up to individual utilities and their communities to decide to make the effort they determine is appropriate for their specific circumstances. (For additional information on the WSWG's diversity of views on the role that regulation should play in water security, see discussion in Chapter III of this document.)

The WSWG recognizes that many utilities use a multi-barrier approach to water and wastewater management. In a multi-barrier approach, multiple barriers covering the full scope of utility infrastructure are chosen in consideration of utility-specific circumstances and operating conditions, and implemented as an integrated, seamless system to protect drinking water services and quality from source water to tap, and to protect wastewater services, from collection through treatment and discharge. Multi-barrier approaches are built on the premise that a combination of efforts throughout a utility will be more robust than reliance on any single tactic or point of influence. The WSWG security findings and the 14 features of an active and effective security program take a similar approach, calling on utilities to understand the specific, local circumstances and conditions under which they operate, and to develop an enterprise-wide security program tailored to those specific circumstances

and operating conditions. In security, this approach is called protection in depth, or security layering. The WSWG encourages utilities that have multi-barrier water and wastewater management approaches to consider how they might build on these approaches to incorporate security layers.

Finally, the WSWG also is very aware that many utilities already have made considerable progress in developing security programs. In this context, the Group was careful to craft its findings to build upon this progress.

II. SECURITY

The first part of the WSWG charge was to "identify, compile, and characterize best security practices and policies for drinking water and wastewater utilities, and provide an approach for considering and adopting these practices and policies at a utility level." Early in their deliberations, the WSWG rejected use of the term "best" to describe their work on security practices. Instead, the Group chose to identify and describe the scope, principles, and features of "active and effective" security programs, and to make a series of related findings on improving the climate for water and wastewater security.

Approach to Developing Findings on Security

The WSWG began deliberations on security practices and programs by considering the current body of security-related guidance. This included preparing a detailed annotated bibliography of security-related references (Attachment 4), reviewing the security literature, and identifying and considering common security-related themes. The WSWG also considered presentations on security from Group members and outside experts. From these initial deliberations, the WSWG identified 12 common interests shared across the Group. The WSWG used these common interests to guide their findings on active and effective security programs and to set the stage on which the Group's security-related findings should be reviewed.

Common interests informed and guided the WSWG's deliberations and created the basis for agreement on substantive findings related to security.

1. Don't reinvent the wheel; understand and use existing information, adding new value.
2. Limit inclusion of security-sensitive information to maximize the utility of the product and ensure it can be distributed and used.
3. Seek to maximize benefits by emphasizing actions that have the potential to both improve the quality or reliability of utility service, and to enhance security.
4. Programs should have measurable goals and timelines.
5. Be attentive to concerns that more clearly defining security practices may create liability concerns, especially for smaller utilities, which may not have the resources to implement all security enhancements immediately.
6. Be aware that, in some jurisdictions, political or organizational interest in security may be diminishing, making it more difficult for utility operators to gain the support and resources needed for security enhancements.
7. Recognize the need to tailor security programs and practices to utility-specific characteristics, such as whether a utility is urban or rural, and whether it is small, medium, or large in size.
8. Recognize constraints and barriers, but do not let them define security findings. For example, where a practice is desirable but implementation is constrained, findings could call for the practice, and recognize and suggest ways to overcome constraints.
9. Address prevention as a key aspect of enhancing security.
10. Emphasize that inherently safer practices or practices that have a lower risk potential also have potential to enhance security.
11. Recognize and manage the relationship between practices that increase safety and those that increase security. Safety and security may complement each other, may be neutral, or may conflict. For example, a supervisory control and data acquisition (SCADA) system provides valuable operating safety

information, but may also introduce a vulnerability that someone could use to cause harm or mislead operators. Similarly, permanently locking a door for security reasons might create a safety barrier to an emergency exit.

12. Develop findings in a way that creates an awareness of security and an understanding of the rationale for findings among water sector stakeholders and the public, and encourage utilities to take a similar approach in developing utility-specific programs, consistent with the need to hold security-sensitive information closely.

Many of the common interests identified by the WSWG to guide the Group's deliberations on security are also suggested by the Group as principles for use by utilities as they develop active and effective security programs (see Finding 4).

Summary of Findings on Security

The WSWG developed eight findings on security. Finding 1 calls for utilities to achieve consistent security outcomes with significant flexibility to tailor security approaches and tactics to utility-specific circumstances and operating conditions. Findings 2 through 4 address the scope of active and effective security programs, significant system failures and key threats that should be considered, and program principles. Finding 5 identifies the features that should be present in all active and effective utility security programs. Finding 6 calls on utilities to use a continual improvement approach to learn from implementation of security programs and enhance security over time. Findings 7 and 8 call for improving the climate for water and wastewater security by improving connections between the utility and public health communities, and improving the reliability and affordability of physical and chemical contaminant monitoring technologies.

One Size Does Not Fit All

Finding 1: Water and wastewater utility security programs should achieve consistent outcomes using utility-specific tactics and implementation approaches that are tailored to individual utilities' circumstances and operating conditions.

The first item the WSWG discussed and agreed upon was the need to provide individual utilities the means to tailor security tactics and approaches to utility-specific circumstances and operating conditions. At the same time, the Group also recognized the need to create clear expectations and promote consistency in security program outcomes. The Group struck this balance using an approach that is centered around suggesting that all utilities address 14 common features of active and effective security programs (detailed in Finding 5), in the context of utility-specific circumstances and operating conditions.

All water and wastewater utilities should address security in an informed and systematic way, consider their specific circumstances and operating conditions, and develop, implement, monitor, and improve specific security tactics to create an active and effective security program appropriate to utility-specific conditions. The WSWG discussed this as defining "what to do" instead of "how to do it." Using this approach, the Group makes findings that describe the scope of active and effective security programs (Finding 2), the significant system failures and key threats utilities should consider (Finding 3), security program principles (Finding 4), and security program features (Finding 5). It is left to individual utilities to determine how best to craft a security program that addresses these findings in a way that is appropriate to their specific conditions.

Water and wastewater utilities come in all shapes and sizes—there are large urban utilities and small rural utilities. There are utilities that rely on ground water and those that rely on surface water. There are utilities with inherently higher-risk operations in higher risk locations or circumstances, and utilities that operate with a lower risk profile. Some utilities have multiple sources of source water and redundant treatment capacity; others do not. Some utilities may have large security budgets, and others may face difficult decisions about setting priorities between security spending and other necessary spending. Political and public support or interest may affect a utility's ability to implement security measures. Legal barriers, especially for public utilities, might affect, for example, utilities' ability to carry out employee background checks or to implement other security approaches. Some vulnerabilities can be as specific as where an extra set of keys is hanging. The possibilities are infinite.

These and other utility-specific circumstances and conditions must inform development of specific security tactics. A rigid approach that requires a certain type of fence or other access control, or a prescribed information technology protection system or standard set of personnel security policies would, automatically, over-address security needs for some utilities and under-address security needs for other utilities. It would under-invest in some places, and over-spend in others. In essence, there is no prescriptive, uniform filter that can be applied to every community in the country to determine if they have established the best possible security tactics and countermeasures—as discussed throughout the document, decisions about utility-specific security tactics and countermeasures should be determined in light of utility-specific circumstances and operating conditions. The WSWG agrees that due respect should be given to priorities established through utility-specific assessments of vulnerability. It would be counterproductive for a uniform perspective of security tactics and countermeasures to override priorities established through utility-specific vulnerability assessments. The WSWG discussed this using the catch phrase "one size does not fit all."

The WSWG recognizes that their approach will result in considerable variability in the specific security tactics and approaches individual utilities implement. Some utilities may—and may need to—create distinct security programs, with new security managers and security staff. Other utilities may appropriately address the program features simply by ensuring existing managers and staff address security concerns as part of their responsibilities. Some utilities may—and may need to—invest heavily in physical hardening of infrastructure and access control. (Physical hardening involves designing-in the means to make a facility harder to attack—or appear harder to attack—and to reduce the effect of any attack that may take place.) Other utilities may rely more heavily on timely intrusion detection and response. This variability is to be expected and is appropriate to the variability inherent in utility circumstances and operations. The WSWG emphasizes that the important outcome is that all utilities, regardless of size or circumstance, should address security in an informed and systematic way; should consider their specific circumstances and operating conditions; and should develop, implement, monitor, and improve specific security tactics to create an active and effective security program appropriate to utility-specific conditions.

Security Program Scope

Finding 2: Active and effective security programs should address protection of public health, public safety (including infrastructure), and public confidence.

After agreeing on the importance of defining security outcomes that all utilities should achieve—and at the same time agreeing on the need to tailor security tactics and approaches to utility-specific circumstances and operating conditions—the WSWG turned to describing the scope of an active and effective security program.

The main outcome of an active and effective security program is to ensure reliable operation of water and wastewater infrastructure, reliable drinking water, and reliable wastewater collection and treatment services. Reliable, clean water is needed for consumption and for the prevention of disease and maintenance of public health; reliable water also is needed for operation of wastewater collection and treatment facilities, and other facilities necessary to public health. Reliable water at sufficient pressure is needed to protect public safety and infrastructure—to fight fires, operate industrial facilities, and cool industrial and other operations. Reliable water treatment is needed to prevent uncontrolled—or untreated or not fully treated—wastewater discharges from fouling beaches, water bodies, and even drinking water supplies, with serious public health, environmental, and economic consequences.

The WSWG discussed which of these adverse consequences active and effective security programs should address, and agreed that protection should be provided across the full range of adverse consequences that might be brought about if a water or wastewater utility were to be compromised. The WSWG defined these as adverse consequences for public health, adverse consequences for public safety, and adverse consequences for public confidence. The Group agreed that active and effective security programs should protect against all these potential adverse consequences, although they recognized some might be more of a concern than others based on utility-specific conditions. For example, when a utility provides the only potential source of water for firefighting, protection of public safety by ensuring the continued reliability of a supply of firefighting water might need special attention. Similarly, interruption of wastewater collection and treatment services for a large metropolitan area is different from interruption of such services for a small town. The Group also discussed the need to avoid adverse consequences, regardless of the means that might bring such consequences about. Whether a water supply is interrupted because of accident, vandalism, or terrorist attack matters less than the actions needed to bring a system back on line. In addition to making water and wastewater utilities safer from attack, active and effective security programs will have the collateral benefit of improving responses to accidents and reducing the impact of natural disasters and vandalism.

The WSWG discussed "protect against" as meaning the design and implementation of utility-specific security tactics and approaches that seek to minimize adverse outcomes by preventing or being well prepared to respond to and recover from an attack or other event, such as vandalism. Active and effective security programs, therefore, will include elements of **prevention** (through access and intrusion detection and control, contaminant detection and monitoring, physical hardening of systems, inherently safer design and construction choices, and controlling access to security-sensitive information), **preparedness** (through having plans and procedures in place and building the successful partnerships and communication mechanisms needed to prevent and respond to an attack), and **response**, **consequence management**, **mitigation**, and **recovery**. Each of these aspects of protection are addressed more fully in the 14 features of active and effective water security programs described in Finding 5.

The WSWG believes that creating and sustaining public confidence deserves special consideration. Many WSWG members who own or operate water and wastewater utilities were particularly concerned about sustaining public confidence. Reliable, safe water is an expectation in the United States. Any real or perceived threat to the safety of the water supply could—even if no sickness or death occurs—have a significant adverse effect on public health and safety, and the economy, by causing customers to mistrust water supplies. Utility operators are very concerned about this potential outcome and about the ability of a utility to effectively recover from a loss of public confidence. Later findings on developing reliable partnerships and on communication contemplate that all utilities will take steps to create and sustain public confidence as part of an active and effective security program.

Significant System Failures and Key Threats

Finding 3: Active and effective security programs should consider six significant system failures and four key threats, as described below.

After discussing the scope of active and effective security programs, the WSWG discussed the specific potential significant system failures that should be guarded against and the types of potential threats that might bring about significant system failures. Key threats are actions that have the potential, individually or in combination, to cause a significant system failure. Significant system failures are those that, should they occur, are likely to disrupt or endanger public health, safety, or confidence. The WSWG identified six significant system failures water and wastewater utilities should consider when developing an active and effective security program.

1. Loss of pressurized water for a significant part of the system.
2. Long-term loss of water supply, treatment, or distribution.
3. Catastrophic release or theft of on-site hazardous chemicals affecting public health.
4. Adverse impacts to public health or confidence resulting from a contamination threat or incident.
5. Long-term loss of wastewater treatment or collection capacity.
6. Use of the collection system as a means of attack on other targets.

The WSWG defined four key threats that water and wastewater utilities should consider when developing an active and effective security program.

1. Physical disruption of core facilities, such as chemical storage, or interdependent infrastructure, such as communication, power, and transportation, either through direct physical targeting or as a result of collateral damage.
2. Chemical, biological, or radiological material used to contaminate water supplies or infrastructure.
3. Cyber attack on information technology assets to disrupt service and/or obtain confidential information.
4. Use of conveyance tunnels or storm, sanitary, or combined sewers to stage an attack against utilities or other targets.

The WSWG emphasizes that these significant system failures and key threats are intended only as a standard set of possibilities a utility should consider when choosing security priorities and tactics for its specific active and effective security program. Consideration of the significant system failures and key threats will inform how utilities set specific security priorities and choose security tactics and approaches, but the lists of major system failures and key threats do not prejudge or demand any particular set of security tactics or approaches.

The exact definition of significant system failure for any given utility also will depend on utility-specific conditions. For instance, what constitutes a "significant" part of a water distribution system may be different for a large urban utility than for a small rural utility. Similarly, whether a system is particularly concerned with the potential for a "long-term" loss of collection or treatment capacity may differ depending on backup or redundant systems, viable temporary alternatives, amount of material collected, and environmental or economic sensitivity of receiving waters.

Some significant system failures and key threats will be more relevant to some utilities than others. For instance, some utilities may be particularly concerned about cyber attack, or use of conveyance

tunnels or storm, sanitary, or combined sewers to attack utility or other targets. Other utilities, because of the nature of their operating systems, or the size or location of their infrastructure, may be less concerned about these potential threats. It is important for utilities to consider the significant system failures and key threats critically, in light of their specific circumstances and operating conditions. For some utilities, other potential significant system failures or key threats may be more important than those mentioned here.

In the context of significant system failures and key threats, the WSWG also discussed transportation of hazardous chemicals, such as chlorine. The Group strongly feels that utilities should be aware of the schedules for hazardous chemicals being transported to their facilities, the amount of hazardous chemicals in transit, and the expected arrival dates. This information should be used to coordinate and collaborate with individuals responsible for hazardous chemical transportation to enhance the security of hazardous chemicals in transit, even as the primary responsibility for security of chemicals in transit remains with the owners/operators of the transportation service.

Principles That Support Active and Effective Security Programs

Finding 4: Active and effective security programs should be built around 11 principles, as described below.

In their deliberations on the scope and features of active and effective security programs, the WSWG identified 11 principles that apply across utility circumstances and operating conditions. These principles should be used by utilities to guide identification of utility-specific security tactics and approaches. They are meant to provide a thematic sense of the types of security tactics and approaches the WSWG believes will be most effective across the widest range of utilities.

Principles of active and effective security programs should be used by utilities to guide identification of utility-specific security tactics and approaches.

1. Security should be part of organizational culture and the day-to-day thinking of front-line employees, emergency responders, and management.
2. A strong commitment to security by organization leadership and by the supervising body, such as the utility board or rate-setting organization, is critical to success.
3. There is always something that can be done to improve security. Even when resources are limited, the simple act of increasing organizational attentiveness to security will reduce threat potential and increase responsiveness. Preparedness itself can help deter attacks.
4. Prevention is a key aspect of enhancing security.
5. Movement towards practices that are inherently safer (i.e., have a lower risk potential) may enhance security.
6. Security programs require ongoing management and monitoring, and an ongoing budget commitment. A continual reassessment model, where changes are implemented over time as experience with security increases, may be useful.
7. Consideration of security issues should begin as early as possible in facility construction (i.e., it should be a factor in building plans and designs).

8. The relationship between practices that increase safety and those that increase security must be recognized and managed. Safety and security may complement each other, may be neutral, or may conflict. For example, a SCADA system provides valuable operating safety information, but also may introduce a vulnerability that someone could use to cause harm or mislead operators. Similarly, permanently locking a door for security reasons might create a safety barrier to an emergency exit.
9. Strong relationships with response partners and the public strengthen security and public confidence.
10. Investment in security should be reasonable considering utilities' specific circumstances. Where threat potential or potential consequences are greater, greater investment likely is warranted.
11. Utilities should create an awareness of security and an understanding of the rationale for their overall security management approach in the communities they serve, consistent with the need to hold security sensitive information (i.e., attributable information about utility-specific vulnerabilities and security tactics) closely.

The WSWG emphasizes that, as with the findings on program scope and features, these principles for active and effective security programs do not prejudge or prescribe specific security tactics or approaches. As discussed earlier in this document, there will be wide variability in security tactics and approaches across utilities, and this variability is appropriate given the range of utility-specific circumstances and operating conditions. Again, the important outcome is that all utilities, regardless of size or circumstance, should address security in an informed and systematic way, consider their specific circumstances and operating conditions, and develop, implement, monitor, and improve specific security approaches and tactics to create an active and effective security program appropriate to utility-specific conditions.

Security Program Features

Finding 5: Active and effective security programs should include 14 features, described below.

From their agreement on the scope and principles of active and effective security programs, and the need to tailor specific security tactics and approaches to utility-specific circumstances and operating conditions, the WSWG turned to defining the common features of active and effective security programs. The idea behind defining common features of active and effective security programs is to provide for consistency in security program outcomes, guide utilities' consideration and selection of specific security tactics and approaches, and create a foundation from which improvements in security can, over time, be measured and described.

The WSWG's findings on features and measures of active and effective security programs are based on a "security layering" approach. They call on utilities to understand the specific, local circumstances and conditions under which they operate, and to develop an enterprise-wide security program tailored to those specific circumstances and operating conditions. The WSWG suggests an integrated combination of utility-specific tactics that address:

- Prevention, through intrusion detection and access control, contaminant detection and monitoring, physical hardening of systems, inherently safer design and construction choices, and controlling access to security-sensitive information;
- Preparedness, through having plans and procedures in place, participating in training exercises for these plans, and building the successful partnerships and communication mechanisms needed to prevent and respond to an attack; and
- Response, consequence management, mitigation, and recovery in the event of an attack.

WSWG findings call on utilities to address security in all elements of utility infrastructure—from source water to distribution and through collection and wastewater treatment—and to consider the full scope of potential significant system failures and key threats against which they must be protected. A security layering approach uses a combination of public involvement and awareness, partnerships, and physical, chemical, operational, and design controls to increase overall program performance. The WSWG emphasizes the security layering approach because the performance of an enterprise-wide, integrated security program will be more robust than the performance of the combination of un-integrated, individual security tactics.

The 14 program features described by the WSWG purposefully define high-level security program outcomes rather than prescribe specific security approaches or tactics. They were selected from many potential features of security programs as those that, in the experience and view of the WSWG, are most important to increasing security and most relevant across the broad range of utility circumstances and operating conditions. The 14 features are listed below.

1. Make an explicit and visible commitment of the senior leadership to security.
2. Promote security awareness throughout the organization.
3. Assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.
4. Identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.
5. Identify managers and employees who are responsible for security and establish security expectations for all staff.
6. Establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.
7. Employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.
8. Define security-sensitive information; establish physical, electronic, and procedural controls to restrict access to security-sensitive information as appropriate; detect unauthorized access; and ensure information and communications systems will function during emergency response and recovery.
9. Incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower-risk design and technology options.
10. Monitor available threat-level information and escalate security procedures in response to relevant threats.
11. Incorporate security considerations into emergency response and recovery plans, test and review plans regularly, and update plans as necessary to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.
12. Develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, and customers.
13. Forge reliable and collaborative partnerships with the communities they serve, managers of critical interdependent infrastructure, and response organizations.
14. Develop utility-specific measures of security activities and achievements, and self assess against these measures to understand and document program progress.

Readers are encouraged to refer to Appendix A for a detailed description of each security program feature. The descriptions include the WSWG's views about how each feature might be implemented, examples of successful implementation strategies, and identification of challenges to overcome.

At a practical level, the point of an active and effective security program is to prepare for, prevent, mitigate, respond to, and/or recover from events that could cause significant system failures, and thereby adversely affect public health, public safety, or public confidence. By necessity, security programs are combinations of layers of mutually supportive, adjustable approaches and tactics that protect people (customers, employees, visitors, and the public who live around plants or other infrastructure); infrastructure (pipelines, aqueducts, plants, structures, equipment, tools, and vehicles); information (employee records, blueprints and diagrams, privileged information, vital records, and details of vulnerabilities); and reputation (consumer confidence and service safety and reliability). Attention to prevention, preparedness, response, consequence management and mitigation, and recovery is needed.

Security programs affect all aspects of utility operation, including human resources, information technology, physical infrastructure, operational functions, customer relations, and coordination with non-utility partners. The features are broadly drawn to allow individual utilities to tailor security approaches and tactics to utility-specific circumstances and operating conditions. At the same time, they are sufficiently important and relevant that they apply across the full range of utility conditions and should be addressed by all utilities. The WSWG emphasizes that significant variability in implementation of the program features is to be expected and is appropriate; however, to have an active and effective security program, utilities should address each feature and develop specific implementation approaches and tactics tailored to their circumstances.

Ongoing Improvement

Finding 6: Water and wastewater utilities should reassess and seek to improve their security programs on an ongoing basis.

Ongoing reassessment and improvement of security programs is important to keep programs "fresh" and effective, and to take advantage of emerging approaches and new technologies. Ongoing reassessment also will increase the effectiveness and efficiency of security programs and organizations over time. In an ongoing reassessment and improvement system, there is regular, explicit evaluation of tactics and approaches, and thoughtful assessment of how these tactics and approaches might be improved. Utilities should undertake regular and explicit evaluation and testing (or exercising) of their security programs, document program failures, and identify program improvements. These evaluations are best undertaken by a team of individuals that includes not only line and executive managers responsible for security, but also line employees who have security-related duties. Implementation of security programs should be thoroughly documented and monitored, so that progress in improving security programs can be identified and evaluated, and further changes and improvements made. At a fundamental level, a system of continual reassessment and improvement reflects the attitude a utility takes towards security. Like developing a security-improvement culture (discussed in Finding 5 and part of features 1 and 2 in Appendix A), successful reassessment and improvement approaches rely on employees at all levels of an organization making a commitment to doing their part to improve security.

A commitment to continual reassessment and improvement is critically enabled by clear, measurable goals for security performance and timelines for achieving this performance. Later in this document, the WSWG suggests a series of measures related to the 14 security program features. These measures form a starting point from which utilities can develop security-related goals.

Improve Connections with Public Health

Finding 7: Relationships between the water and wastewater utility sector and the public health sector should be strengthened.

Historically, connections between water and wastewater utilities and the public health community have tended to be ad hoc. Water and wastewater utilities and public health organizations need to develop stronger working relationships so they are better prepared to detect problems, respond, and recover in the event of an emergency. Opportunities for collaboration between water and wastewater utilities and public health agencies should be provided through commitment to regular communication, and ongoing joint training, planning, and exercises.

It also is important for utilities and public health organizations to plan together for consistency of messages in a utility-related emergency. For example, utilities and public health organizations should develop consistent messages and planning around the potential for boil water advisories and orders, so that the public will receive consistent information about how and when to boil water, from both the utility and the public health community. Coordination is important at all levels of the public health community—national public health, county health agencies, and health-care providers, such as hospitals.

Information sharing between utilities and public health agencies can enhance detection and response. For example, increased complaints to water utilities or public heath agencies could indicate a problem, when coupled with other public health surveillance data or routine water quality monitoring data. Given current limitations on physical and chemical monitoring technologies, attention to public health data may be the main form of contaminant detection and monitoring for water-related health problems.

It may be helpful for utilities and public health organizations to establish formal agreements on coordination. These agreements could ensure regular exchange of information between utilities and public health organizations, and outline roles and responsibilities during response to and recovery from an emergency.

Support Development of Contaminant Monitoring Technologies

Finding 8: Development and distribution of reliable, affordable contaminant monitoring technologies is important to improving utility security, and should be facilitated and supported by government.

In the features of an active and effective security program, the WSWG calls on utilities to employ protocols for detection of contamination consistent with the recognized limitations in current contaminant monitoring technologies. Currently, utilities' ability to undertake chemical, biological, and radiological monitoring of contamination is limited in large part by the lack of reliable or affordable technology, and the lack of guidance or experience to interpret monitoring results. While development of guidelines, instruments, and methodologies for chemical, biological, and radiological monitoring for contamination is already an evolving area of research, more progress is needed to provide for more direct and real time methods for contaminant monitoring and interpretation of monitoring data. The WSWG strongly encourages government to continue and increase financial and other support for the development of chemical, biological, and radiological monitoring technologies, and to assist utilities in creating protocols and guidelines for interpretation of contaminant monitoring data.

III. INCENTIVES

The second component of the mission given to the WSWG by the NDWAC was to "consider mechanisms to provide recognition and incentives that facilitate a broad and receptive response among the water sector to implement best security practices and policies, and make findings as appropriate."

Approach to Developing Findings on Incentives

The WSWG began deliberations on incentives by considering what an incentive is. The Group discussed that incentives are created by identification of desired behaviors and desired benefits. If the desired behavior is broad implementation of active and effective security programs, incentives will come from identification of the benefits, or reasons that might motivate utility owners/operators to implement and maintain active and effective security programs.

The WSWG emphasizes that because of the nature of the utility business and the responsibilities of utility owners/operators relative to public health and safety, most utilities are motivated to implement active and effective security programs as part of their commitment to serving their customers and communities by providing clean, reliable water and reliable sanitary services. Most utilities see themselves as implementing a public trust and take these responsibilities very seriously. Most utility owners/operators and their families live in the cities and towns that they serve, and have a deep commitment to furthering safe, healthy communities. At the same time, the WSWG recognized that even with this motivation, resources in utilities are not unlimited, and time, attention, and capital investment in security improvements must compete against other priorities. As the immediacy of the September 11, 2001 attacks fades with time, attention to security may also wane in the absence of substantial efforts to promote its urgency.

The WSWG discussed incentives as a way to help security improvements remain of high concern and compete more effectively for attention and funding against other utility priorities. In this context, the WSWG identified several benefits that, if available, could prompt utilities to develop and maintain active and effective security programs.

- More efficient/effective operations through inherently more productive practices, and implementation of actions that improve the quality or reliability of utility service, and enhance security.
- A more safe and secure working environment and community.
- A more solid, comprehensive business plan.
- Better understanding and support in the community, which may help rate payers tolerate higher rates that correspond to safer operating conditions.
- Potential reduction in liability, with the potential for resultant reductions in insurance costs or premiums, by demonstrating actions consistent with industry guidelines for active and effective security programs. Conversely, if an active and effective security program is not implemented, liability may increase. (Note, the WSWG did not carry out extensive consultations with the insurance industry; EPA should consider such consultation as a way to further explore the role the insurance industry might play in providing incentives for active and effective security programs.)
- Regulatory flexibility might be offered if, for example, a permit or regulatory violation occurs as a consequence of a successful attack.

- More reliable and trusted utility performance and products, increasing community approval ratings and public trust.
- If available, financial support for implementation of security improvements.

The WSWG also discussed that establishing clear expectations for security, such as those established by the WSWG's findings on features and measures of active and effective security programs, is, on its own, a powerful motivator for utilities to take action. Clear expectations set an industry benchmark and a potential basis against which decision makers within utility organizations, oversight agencies, financial and insurance markets, peers, customers, and the public can evaluate progress. It is important to continue to emphasize clear expectations for outcomes of active and effective security programs—to create a yardstick against which utilities can measure themselves and to establish expectations about performance industry wide. As noted in the first finding on incentives (see Finding 9), the potential for increased liability in the event that a utility fails to adequately address security and an attack or other event interrupts utility services, injures people or property, or otherwise causes harm, is a powerful motivator for action.

Summary of Findings on Incentives

The WSWG developed a number of findings on incentives. Finding 9 addresses the need to reinforce the importance of active and effective security programs and the potential for negative consequences if security is not addressed. Finding 10 addresses recognition of security programs. Finding 11 calls on EPA and others to establish a peer review system for utility security. Findings 12 and 13 address technical assistance and other support for utility security efforts, and findings 14 and 15 address funding for security by calling for direct financial support and for education for utility oversight boards and rate-setting agencies.

Understanding the Consequences of Failing to Address Security

Finding 9: EPA, DHS, state agencies, and water and wastewater utility organizations should provide information on the importance of active and effective security programs to utilities, and should make owners and operators more aware of the benefits of active and effective security programs and of the potential negative consequences of failing to address security.

Information is a powerful motivator for action. In the utility community, trusted information comes largely from utility organizations such as the American Water Works Association (AWWA), the Water Environment Federation (WEF), the National Association of Clean Water Agencies (NACWA), the Association of Metropolitan Water Agencies (AMWA), and the National Rural Water Association (NRWA). Federal and state agencies and officials also have a role to play in providing information. Because utilities have many priorities and competition for resources may be great, it is important that security remain a high-profile concern.

While positive reinforcement of the importance of active and effective security programs may provide adequate motivation for many utilities that are already interested in improving security, it is also necessary to ensure that utilities have information about the potential negative consequences of failing to address security. For utilities that are not yet motivated to address security, information on the potential negative consequences of failing to act may be the factor that prompts them to begin to take action. The WSWG identified a number of potential negative consequences of failing to address security; these include increasing the potential for attack, vandalism, or other interruption to utility services by making the utility an "easy" target; reduced response capabilities in the

event of an emergency; and potential liability if an attack or other event interrupts utility services, injures people or property, or otherwise causes harm. The WSWG discussed increased liability in particular as one of the key negative consequences of failing to address security needs.

Information on the benefits of an active and effective security program and the potential negative consequences of failing to address security also will raise public awareness of utility security issues and may thereby increase public support for utility security efforts. Utilities are very interested in what the public—their customers—want, and are very concerned about maintaining high levels of public support. Public pressure and support for security improvements will assist utilities that are already taking steps to address security by providing another argument in support of security investments, and may serve as further motivation for utilities that have not yet addressed security issues.

Recognition

Finding 10: EPA, DHS, state agencies, and water and wastewater utility organizations should develop programs and/or awards that recognize utilities that develop and maintain active and effective security programs, and that demonstrate superior security performance.

Peer pressure and peer recognition are important in any profession. In the utility community, owners and operators tend to be highly aware of the accomplishments of their peers and attuned to peer recognition. Programs like the Partnership for Safe Water, the National Biosolids Partnership, the AWWA Exemplary Source Water Protection Award and Public Communications Achievement Award, the NACWA Peak Performance Award, the NRWA Excellence Awards, and the AMWA's Gold and Platinum awards for Competitiveness Achievement and Sustained Competitiveness serve to motivate utility action and recognize high achievement. Awards such as these can improve utilities' standing in their communities, and increase public support and trust.

By developing awards focused on security performance and improvement, EPA and water and wastewater utility organizations will continue to raise the profile of security in the utility industry, reinforce the importance of developing and maintaining active and effective security programs, and motivate utilities to enhance and accelerate security improvements. As award and recognition programs are developed, it will be important to remain sensitive to potential risks associated with calling attention to security performance—in particular, some members were concerned that security awards could make award-winning utilities more attractive targets by drawing attention to them. This concern might be mitigated by incorporating security considerations as an additional element of existing award programs that recognize overall superior performance, rather than developing stand alone security awards. Recognition also might be provided by inviting utilities to participate as peer reviewers or experts in a utility security peer review program. Award and recognition programs also should recognize that in some cases, the changes to utility operations needed for active and effective security programs are more extensive—and may be more difficult to bring about—than the types of operational changes or performance addressed by existing utility award programs.

Peer Assistance and Review

Finding 11: EPA, DHS, state agencies, and water and wastewater utility organizations should support development and implementation of a voluntary utility security peer technical assistance and review program.

As discussed in Finding 12 on technical assistance, forging connections between peers is a highly effective means to deliver support. Programs that offer technical assistance, training, or circuit rider assistance, such as those offered by the Rural Community Assistance Partnership (RCAP), the NRWA, and states often succeed because they rely on individuals with similar backgrounds and responsibilities working together to learn from one another. For example, in 2000, the Dade County Water & Sewer Authority worked with the Georgia Rural Water Association (GRWA) to develop the GRWA Small System Peer Review Team. The team matches experts from small, rural water systems that have information or advice to share with small systems that need help. What began in Georgia has now spread to Kentucky, Mississippi, Virginia, and tribal governments on the East Coast, with remarkable results. In Georgia, safe drinking water compliance rates have climbed from 73 percent before the program to 96 percent today.

A utility security peer technical assistance and review program could motivate utilities to seek help in developing active and effective security programs by delivering help in a way that is practical, easy-to-use, and respected. Programs, such as those put in place by the RCAP, NRWA, the GRWA Small System Peer Review Program, and the QualServe Self Assessment and Peer Review Program, can serve as models for successful peer approaches.

In addition to helping utilities put active and effective security programs in place, a successful peer review program can increase confidence in utility security programs. Earlier in this document (see feature 14), the WSWG suggested that active and effective security programs should include utility-specific measures of program achievement and regular self assessment. Peer review could be an important complement to utility self assessment by offering confirmation of self assessment findings or alternative views and advice on needed security improvements.

Technical Assistance

Finding 12: EPA, DHS, state agencies, and water and wastewater utility organizations should help utilities develop active and effective security programs by providing information on different types of technical assistance, including technology verification information.

Where utilities are already motivated to address security issues, technical assistance programs can provide the critical added expertise or support needed to make good intentions towards security a reality. Where a utility is not yet motivated to address security issues, technical assistance can provide the support needed to make security approachable enough to overcome resistance. Currently, there are many effective technical assistance programs and resources designed to assist utilities in their efforts to comply with the requirements of the Bioterrorism Act of 2002 and to improve water and wastewater security. These include EPA documents, such as the Response Protocol Toolbox; ongoing training and assistance efforts offered by states, EPA, and utility industry associations; circuit rider programs, such as those put in place by the NRWA and the RCAP; ongoing federally-funded research into security approaches and products; and comparative information on security products, such as the EPA Security Product Guides, and online, accessible libraries of information on contaminants and other security-related topics, such as the WaterISAC. It is important that these efforts continue and be expanded.

In particular, utilities would be helped in their efforts to implement active and effective security programs by reliable, practical information on the performance capabilities of various security technologies. As security has become a higher-profile concern in the utility industry, a proliferation of security vendors has come forward to market a vast array of security-related tools and technologies. Independent verification of the performance of these tools and technologies, such as that provided through EPA's Technology Testing and Evaluation Program (TTEP) would be a valuable incentive to utilities and would help ensure that utilities get the most benefit from their investments in security. The primary focus of the TTEP program is the testing of commercially available technologies, with a keen eye toward the end users' security needs. Homeland security technologies for detection, monitoring, treatment, decontamination, computer modeling, and design tools will be tested against a wide range of performance characteristics, requirements, and specifications. Performance results will be reported in testing summaries and in side-by-side comparisons between products. To complement programs such as TTEP, programs that promote technology evaluation and testing before verification efforts also are needed.

Utilities also would be helped by information on options for choosing inherently safer designs and technologies, and how to factor consideration of inherent safety into design and technology decisions. Inherently safer designs and technologies reduce the overall risk potential associated with an activity. The choice of which technology or design to use will involve consideration of numerous factors, including utility-specific circumstances and operating conditions, hazards and hazard potential, resources, security and other utility priorities, and which technology or design offers the most inherent safety or robust performance. As described in Finding 5, feature 9—moving towards inherently safer designs and technologies is desirable as a way to reduce the potential harmful consequences of a successful attack on a utility, natural disaster, or other event.

In providing technical assistance, EPA and water and wastewater utility organizations should keep in mind that different types of assistance may work better for different utilities, depending on utility-specific circumstances and operating conditions. For example, smaller utilities without staff specifically dedicated to security might be best helped through question and answer hotlines, in-person assistance and training, or periodic workshops. Larger utilities with security staff may be able to make better use of studies, guidance documents, or other approaches.

The WSWG emphasizes that regardless of the type of technical assistance, there are three important elements of technical assistance that should be considered as this finding is implemented.

- First, assistance must be relevant to the receiver. EPA and others should reach out to the utility community to ascertain what information, tools, and training they would find most valuable. This should recognize that the needs of large utilities likely are different from the needs of small utilities, and that tailored, or different, materials may be needed for different audiences.
- Second, assistance is best received when it comes from a respected peer. Every effort should be made to involve utilities and their peers in developing and providing technical assistance to each other. Circuit rider and technical assistance programs, such as those put in place by RCAP and NRWA, and peer review programs, such as the Small System Peer Review Team and the QualServe Self Assessment and Peer Review Program, succeed because they rely on individuals with similar backgrounds and responsibilities working together to learn from one another.
- Third, assistance materials must be easy to use and accessible. The vast majority of utilities are small systems that do not have staff specifically dedicated to security and will have limited time, attention, and resources to devote to security. It is critical that technical assistance information be well organized, clearly written, and focused on practical, implementation-oriented steps that utility operators can take to improve security. Whenever possible, checklists, tables, or other devices should be used to provide information in an

easily accessible way. No one has time to pore through a fifty-page document to find the information relevant to them. In particular, utilities would be helped by easy-to-use information about effective security program approaches and tactics; case studies; model and/or example policies, procedures, templates and agreements; checklists; and other practical information. EPA and states should consult further with utilities to understand what types of technical assistance programs and documents are currently considered helpful and should build upon, support, or replicate successful models.

For example, small communities have generated a model that has proven highly effective—the Security and Environmental Management System (SEMS). This software was developed in consultation with state drinking water administrators and has been approved by EPA as an acceptable methodology to use for vulnerability assessments. The SEMS software has been distributed to small communities with training for relatively no charge and has been updated by the U.S. Department of Agriculture for wastewater systems. Many small communities that have conducted vulnerability assessments used the SEMS model. As discussed above, the WSWG believes it will be useful for EPA to examine the appeal and effectiveness of the SEMS approach and other technical assistance approaches and programs to inform future technical assistance efforts.

Access to Security-Related Support and Planning

Finding 13: EPA, DHS, and other federal and state agencies should support utility security programs by helping utilities obtain access to needed security-related support systems and infrastructure, and by supporting inclusion of utilities in security exercises.

For utilities to succeed in improving security, they need to become an integral part of the web of security-related improvements that have been put into place since the terrorist attacks of September 11, 2001. Including utilities in this way will directly improve utility security; reinforce the idea of security partnerships between utilities, law enforcement, and first responders; and improve communication between utilities and their partners. In particular, utilities need access to secure joint incident command communication technologies and related security communication bandwidth, and they need to be part of law enforcement's planning for communications in the event of an emergency.

Utilities also should take an active role in collaborative partnerships and mutual aid and mutual assistance agreements. An example of the latter is the Water and Wastewater Agency Response Network, which provides reimbursable mutual assistance and indemnification for water and wastewater agencies throughout California. Similarly, representatives of Milwaukee Water Works, the Milwaukee Health Department, the Department of Public Works, Milwaukee Metropolitan Sewerage District, State of Wisconsin Division of Health, and Wisconsin Department of Natural Resources meet monthly in a Water-Health Technical Committee to exchange information, review watershed testing and epidemiological reports, and discuss shared water quality and health goals.

Finally, utilities should be part of local and regional disaster and emergency response planning and preparation, and should be included in joint tabletop and other exercises (such as the TOPOFF3 exercise completed in spring 2005). This inclusion will foster testing of utility security approaches and tactics, and encourage closer connections, better communication, and partnership with law enforcement, public health, and other first responders. In surveys carried out by the Government Accountability Office, drinking water and wastewater experts identified support for utility participation in emergency response planning and exercises and strengthening key relationships between water utilities and other agencies with emergency response roles as one of the key areas where federal support, including financial support, is needed. (See, *Drinking Water: Experts'*

Views on How Future Federal Funding Can Best Be Spent to Improve Security (GAO-04-29, October 2003) and *Wastewater Facilities: Experts' Views on How Federal Funds Should Be Spent to Improve Security* (GAO-05-165, January 2005).)

Financial Support

Finding 14: Congress, EPA, DHS, and other federal agencies should support security enhancements with grant and loan programs focused on security.

Federal government spending on security has increased dramatically since September 11, 2001. The federal government supports utility investments in security by providing grant support to states' public health, emergency preparedness and response, and environmental agencies, and by providing grant and other support to utility industry associations, research institutions, and others to support training, technical assistance, and development of assistance tools for water security. It is important that this financial support continue and expand, and that funds are focused on efforts that directly support utility security improvements and are made available to all utilities regardless of ownership status. The WSWG particularly supports direct grants to utilities to assist with security improvements.

To complement support for security, EPA and other federal agencies also should increase funding in existing financial assistance programs, such as the Drinking Water State Revolving Fund and the Wastewater State Revolving Fund (loan funds for improvements to drinking and wastewater infrastructure), so that funds are available for all critically needed improvements, including security improvements. The WSWG acknowledges that, as a practical matter, given the current under-funding of the Drinking Water State Revolving Fund and the Clean Water State Revolving Fund, it is difficult (if not impossible) to fund investments needed to improve water quality and meet new maximum contaminant limit standards in a timely way, let alone fund security. The WSWG emphasizes that new, increased, directed funding for the Drinking Water State Revolving Fund and the Clean Water State Revolving Fund is needed if they are to be considered practical methods of security funding. The Group emphasizes the need for new resources dedicated to security—it is not the Group's intention for federal agencies to simply shift funding from existing water programs to water security, or to simply re-prioritize spending from the Drinking Water State Revolving Fund or the Clean Water State Revolving Fund.

In surveys carried out by the Government Accountability Office, drinking water and wastewater experts identified specific areas where financial support for security improvements are needed; see *Drinking Water: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security* (GAO-04-29, October 2003) and *Wastewater Facilities: Experts' Views on How Federal Funds Should Be Spent to Improve Security* (GAO-05-165, January 2005).

Rate-Setting Organizations

Finding 15: Utility governing bodies should recognize costs associated with implementing active and effective security programs. EPA, DHS, state agencies, and utility organizations should provide educational and other materials to boards and rate setting organizations to help them understand security costs.

For most utilities, rates are set by or in consultation with a governing body. Public utilities generally have boards or other oversight organizations that are responsible for rate setting. Private utilities generally are overseen by state utility commissions or other rate-setting organizations. These governing bodies must balance many considerations in determining allowable utility rates, and must form opinions about how much money and other resources are needed to operate a utility, when capital improvements are needed, as well as other needs. Because security improvements can represent significant capital investments, and because development of active and effective security programs, even where capital investments are not needed, requires resources, it is important that utility oversight boards and rate-setting organizations are aware of and provide for timely, appropriate recovery of security costs. Although rate-setting organizations need reasonable information to document security costs, for information security reasons, the amount and nature of the information provided to rate-setting organizations to support increases in rates must be balanced and managed.

Regulation

When EPA announced the formation of the WSWG, the Agency expressed its intention to facilitate "the development of voluntary best security practices." In the Group's deliberations, when the topic arose, EPA reiterated its intention to move towards voluntary standards or guidelines for active and effective security programs. NDWAC members who served on the WSWG also indicated that the WSWG's charge from the NDWAC was formulated in the context of voluntary rather than regulatory efforts. In spite of this emphasis on consideration of voluntary standards, the topic of regulation did arise during the WSWG's deliberations.

WSWG members have a range of views about the use of regulations as a way to motivate implementation and maintenance of active and effective security programs. Some members believe that well-crafted regulations would be a powerful and appropriate motivator. Members who support regulations believe that regulations could be developed that establish the broad outlines and expectations of utility security programs, and acknowledge the importance of providing significant flexibility for individual utilities to design programs and choose security tactics that are practical, given utility-specific circumstances and operating conditions. Members who support appropriate regulation observe that, without regulation, it is increasingly difficult for security implementation priorities to compete for attention and funding against priorities that do have a regulatory mandate.

Some other members are not supportive of regulation. Members who do not support regulation believe that regulations are not necessary to prompt utilities to implement and maintain active and effective security programs. They note the significant investments in security already made by water and wastewater utilities, and further observe that, given this progress, any regulatory effort would likely result in some utilities having to re-do security programs that are already in place and functioning well. Members who do not support regulation believe that it would be difficult to craft sufficiently flexible regulatory frameworks that could accommodate the types of significant flexibility in utility-specific security approaches and tactics that utilities need, and that regulations would tend to create a "one-size-fits-all" approach.

Regardless of their views on regulation, WSWG members agree that it is important for utilities to step up to the challenge of voluntarily implementing active and effective security programs.

IV. MEASURES

The third component of the mission given to the WSWG by the NDWAC was to consider mechanisms to measure the extent of implementation of these best security practices and policies, identify the impediments to their implementation, and present findings as appropriate. WSWG deliberations focused on mechanisms to measure the extent of implementation of active and effective security programs at individual utilities and throughout the water sector.

Approach to Developing Findings on Measures

In deliberations about measures, the WSWG was guided by a number of key concepts.

- As a starting point, measures must help individual utilities to better understand their own performance relative to the features of active and effective security programs.
- Walk before you run—in the beginning, simple, binary (e.g., yes/no) measures focused on activities may be appropriate at some utilities; over time, utilities should strive for measures of program achievement, outcomes, and performance.
- Strict comparability across utilities is not supportable for all measures at this time.
- You need to know what you plan to do before you can measure it—clear security policies, plans, and priorities are important precursors to effective measurement.
- Who will measure, who will use the measure, and how it will be used are important to the acceptance of the measure by utilities, and the ability of customers and the public to trust measurement results.
- A measure's baseline should not penalize proactive organizations.
- Developing and tracking a measure should not compromise security.

From these key concepts, the WSWG developed a three-part approach to measures. First, as discussed earlier in this document and in Appendix A (see Finding 5, feature 14), the Group suggests that water and wastewater utilities develop utility-specific security program measures that reflect those security approaches and tactics the utility has chosen. In Appendix C, the Group lists a number of measures that utilities should consider when developing utility-specific measurement programs. While they will not be applicable to all utilities, the measures listed in Appendix C represent the WSWG's best thinking on a menu of sound measures from which utilities might choose.

Second, the WSWG identified a number of particular measures that address critical security needs and apply regardless of utility size or circumstances. These measures are listed in Finding 16 and represent the minimum necessary for credible self-assessment and measurement.

Third, the WSWG identified three measures that, when reported by individual utilities and aggregated nationally, hold the potential to provide a practical basis for understanding and evaluating sector-wide security progress.

Attributes of Sound Measures

As part of their deliberations, the WSWG discussed and identified eight attributes of a "sound" measure, as follows.

- *Objective*. More objective items make better measures than subjective items.
- *Measurable*. Items that can be measured by standard, accepted methods or devices—with standard units of measure—are better than items that have less accepted or non-standard methods or devices of measurement.
- *Defined*. Items that use standard, well understood definitions of key terms make better measures than items where key terms are less defined.
- *Trackable*. Items that support tracking changes in performance over time against a stable baseline make better measures than items that do not have a stable baseline or cannot be tracked over time.
- *Relevant/useful*. Items that are relevant and useful to day-to-day operations, core business functions, and the utilities that are expected to gather and use the measurement data make better measures than items that are less relevant to utility operations. Measures that speak to program achievement or performance generally are more relevant and useful than measures of program activities.
- *Specific*. The more specific the item being measured, the better.
- *Communicable/understandable*. Items that can be easily communicated and understood within a utility, and to external partners and the public, make better measures than items that are more difficult to communicate to non-utility audiences.
- *Generalizable/comparable*. Items that can be compared among utilities or aggregated to describe sector-wide progress make better measures than items that cannot be compared or generalized.

The WSWG discussed the attributes of sound measures as broad indicators or preferences, rather than strict criteria. The Group recognized and was comfortable that (1) there is considerable overlap among attributes, and (2) not all measures described or suggested by the Group will exhibit all attributes of sound measures. The attributes of sound measures are considerations that the Group used in identifying, describing, and suggesting measures; however, the Group may describe or suggest measures that do not exhibit all the attributes of sound measures.

Types of Measures Considered

The WSWG considered two types of measures: measures of <u>activity</u> and measures of <u>achievement</u>. Measures of activity generally address inputs to a security program—that is, they consider whether a utility has addressed each feature of an active and effective security program by conducting program activities, such as establishing policies and procedures, assigning responsibilities, and conducting activities (e.g., inspections, training, drills). The WSWG believes a sense of security outcomes/achievement can be inferred from activity measures, because activity measures assess the extent to which utilities are paying attention to security issues and the extent to which utilities have addressed the features of active and effective security programs.

Measures of achievement generally address the results of activities—that is, whether the way utilities have addressed individual features of an active and effective security program have actually improved utility security. Achievement measures address whether and how activities are working to achieve program goals or outcomes. The Group believes both measure types are valuable and appropriate for water and wastewater security programs.

Summary of Findings on Measures

The WSWG presents three findings on measures. Finding 16 identifies measures that apply regardless of utility-specific security tactics and approaches, and establishes the expectation that all utilities will include these measures in their utility-specific measurement programs. Finding 17 encourages utilities to consider the list of sound measures that the WSWG developed when establishing utility-specific measurement programs. Finally, Finding 18 addresses national, aggregate measures of sector-wide security progress and considerations, such as verification and consistency, related to implementation of national, aggregate measures.

Minimum Measures Utilities Should Use

Finding 16: At a minimum, utility self assessment and measurement should include 13 measures, described below.

Earlier in this document (see Finding 5), the WSWG identified and suggested that utilities address 14 features of active and effective security programs. In feature 14, the WSWG suggests that utilities should develop utility-specific measures of security activities and achievements, and should self assess against these measures to understand and document program progress. In Finding 16, the WSWG identifies a set of measures of security activities and achievement that should form the basis of a utility-specific self assessment and measurement program. These are measures that the Group believes will be useful across the full range of utilities, regardless of utility size, circumstance, or operating conditions.

- Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?
- Are incidents reported in a timely way and reviewed, and are lessons learned from incident responses incorporated, as appropriate, into future utility security efforts?
- Are reassessments of vulnerabilities made after incidents, and are lessons learned and other relevant information incorporated into security practices?
- Are security priorities clearly identified and to what extent do security priorities have resources assigned to them?
- Are managers and employees who are responsible for security identified?
- To what extent are methods to control access to sensitive assets in place?
- Is there a protocol/procedure in place to identify and respond to suspected contamination events?
- Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how do control measures perform under testing?
- Is there a protocol/procedure for incorporation of security considerations into internal utility design and construction standards for new facilities/infrastructure and major maintenance projects?
- Is there a protocol/procedure for responses to threat level changes?
- Do exercises address the full range of threats—physical, cyber, and contamination—and is there a protocol/procedure to incorporate lessons learned from exercises and actual responses into updates to emergency response and recovery plans?
- Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns?
- Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, public health officials and providers, and response organizations been established?

The measures identified here are not the only measures a utility might use in their self-assessment and measurement program; rather, they are specific aspects the WSWG believes are critically important and apply regardless of utility size, circumstance, or operating conditions. In suggesting these measures, the WSWG acknowledges that utility-specific circumstances and operating conditions and the dynamic nature of security programs may make other additional measures appropriate for an individual utility. The WSWG suggests additional measures for utilities to consider below (see Finding 17), and further acknowledges that individual utilities might identify additional measures not identified by the WSWG. They are, in large part, activity measures. They consider whether a utility has addressed each feature of an active and effective security program through program activities, such as establishing policies and procedures, assigning responsibilities, and conducting inspections, training, and drills associated with each feature. Over time, it may be desirable for water sector stakeholders to work further with EPA and other federal agencies and stakeholders to develop supplemental measures more specifically focused on program achievement and outcomes.

The measures identified by Finding 16 are specifically tied to each feature of active and effective security programs. They describe the minimum effort necessary for measurement and self assessment. Each is phrased as a question. In some cases, the answer may be a simple yes/no; in others, more information may be needed. The WSWG emphasizes it is suggesting these measures as part of utility-specific self-assessment programs. In other words, the only audience for these measures is the utility doing the measuring and anyone the utility elects to share information with. (For example, a utility might elect to share measurement information with a peer reviewer in the context of a voluntary peer review.) Utilities should use these measures to candidly and thoughtfully evaluate their security performance, and to identify opportunities to further improve their security posture.

Readers are encouraged to refer to Appendix A for a discussion of each feature and measure. These discussions include the WSWG's views about how each feature might be implemented, examples of successful implementation strategies, and identification of challenges to overcome. The table in Appendix B shows the suggested features of an active and effective security program and the associated suggested measures.

Note that, consistent with their early agreement that "one size does not fit all" and in recognition that utilities will develop specific security approaches and tactics appropriate to individual utility circumstances and operating conditions, the WSWG decided not to suggest strict comparability of measurement results among utilities at this time. The Group discussed examples of other industries that have developed strict comparability across installations—such as the nuclear power industry—and recognized that the water utility sector does not have the commonalities of quantitative methodology for risks and benefits, standardized analyses on assets to be evaluated, level of detail and evaluation parameters, probability of occurrence of design basis threats, and agreed-upon reliability and failure probability data of various security approaches and tactics that tend to support strict comparability.

Measures for Utilities to Consider

Finding 17: In developing their self-assessment and measurement programs, water and wastewater utilities should consider the security program measures listed in Appendix C.

During their deliberations to identify measures that all utilities should use, the WSWG identified numerous other potential measures of active and effective security programs. The measures suggested above for all utilities to use are the minimum necessary to create a foundation for a successful utility security self-assessment and measurement program. Utilities should supplement the measures suggested above with additional measures

that reflect the specific security approaches and tactics they have chosen. In Appendix C, the WSWG lists measures considered during its deliberations. Utilities should consider these measures when developing a utility-specific self-assessment and measurement program. While not all the measures listed in Appendix C will be applicable to every utility, they cover many of the elements of a successful measurement program that the WSWG suggested earlier (existence of program policies and procedures, training, testing/exercising, and implementing schedules and plans; see feature 14) and represent the WSWG's best thinking on what would constitute sound measures. The list of measures in Appendix C is not comprehensive. It is based on the best thinking of the Group about sound measures for utilities to consider; however, utility-specific circumstances and operating conditions and the dynamic nature of security may make other measures, not listed, more appropriate for individual utilities.

National Aggregate Measures

Finding 18: In considering measurement of water sector security progress, EPA should consider three national, aggregate measures, described below.

After exploring and identifying measures all utilities should use, the WSWG explored measures of national, sector-wide, aggregate progress. The Group discussed two facets of national aggregate measures, the substantive basis for measurement and the measurement process.

The Group agreed that the 14 features and associated core measures of active and effective security programs (see Findings 5 and 16) should serve as the primary substantive basis for measurement. From this discussion, the Group identified three potential national, aggregate measure areas:

- Progress implementing "active and effective" security programs;
- Progress reducing security risks; and
- Progress reducing the inherent risk potential of utility operations.

The Group believes that the first two measures can be supported by data that all utilities with active and effective security programs will have. The measure on reducing the inherent risk potential of utility operations relies on two data sources. The first part of the measure relies on data already reported under the Clean Air Act Section 112(r) and would only affect utilities that are already required to report under this Section—there would be no new reporting. The second part of the measure on reducing the inherent risk potential of utility operations would rely on new data. Each potential national, aggregate measure is discussed in more detail below.

With respect to the measurement process, the Group agreed that:

- Participation in a national measurement program, like development of an active and effective security program, is voluntary; and
- Results of national aggregate measures should be presented only in aggregated form and issues associated with the need for data confidentiality (if any) should be fully addressed before any national measurement program is put into place.

From these agreements, the Group focused on verification of measurement results and consistency in the underlying methods and assumptions that utilities use to establish active and effective security programs. The Group converged around the idea of a phased approach to a measurement process. In the first phase, the national aggregate measures would be based on individual utilities' self assessments of their security programs.

Finding 5, feature 14, calls on utilities to carry out yearly self assessments of their security practices and progress as part of active and effective security programs.

In a potential second phase, self-assessments would be complemented by additional, more independent assessments that could increase the consistency in how progress is reported and have the potential to enhance the overall credibility of national aggregate measures. As follow-up to the WSWG process, EPA should work with the water sector and other interested stakeholders to explore and evaluate additional ways utilities might voluntarily enhance or complement their self assessments. The Group identified a number of potential enhancements or complements to self assessment for further exploration, including peer review approaches, second- and third-party verification approaches, blind or other survey techniques, and incorporation of security programs into utility capacity demonstrations. These and other options should be fully explored. The WSWG does not presume that all of these options will be found to be appropriate. For example, some members have concerns about third party verification, including lack of independence of third party verifiers, lack of standards to qualify third party verifiers, lack of transparency and oversight, and lack of resources for some small utilities to engage third party verifiers. Other members are concerned that variability in utility-specific circumstances and operating conditions will make any assessment process that moves beyond self assessment impractical. Still other members are less worried about third party verification, believing that with a clearly defined focus, and dedicated resources to implement them, independent assessments could increase consistency in how progress is reported and enhance the overall credibility of national aggregate measures.

The WSWG discussed comparability and consistency at some length. The Group agreed that strict comparability between security tactics and approaches at individual utilities is neither necessary nor desirable given the diversity of utility-specific circumstances and operating conditions and corresponding variation in utility-specific security tactics and approaches. For example, comparing specific security program tactics and approaches in Phoenix, AZ to Shelton, WA, and making a judgment about which utility has made more progress is not necessary or desirable. This is consistent with the WSWG's earlier agreement that "one size does not fit all" in utility security.

The WSWG also agreed that as part of exploring measurement processes that might complement self assessment, there may naturally be some exploration of consistency in the methods utilities use to identify threats, assess risks, and prioritize improvements, as these methods will influence the nature of the security programs that utilities adopt and, therefore, the results of any assessment of utility progress. The Group believes that as part of exploring complements to self assessment, EPA, the water sector, and other stakeholders should consider how to detect undesirable variability (if any) in the sector's fundamental methodologies, and, if undesirable variability is identified, consider means to work with the sector to achieve a more appropriate level of consistency. The WSWG emphasizes that this does not contemplate a need for consistency in utility-specific security approaches and tactics. As discussed throughout this document, there will be considerable and appropriate variation in utility-specific security approaches and tactics, to correspond with the considerable diversity of utility-specific circumstances and operating conditions. In any exploration of complements to self-assessment and consistency, EPA, the water sector, and other stakeholders should explicitly consider the idea that different types of utilities might benefit from different approaches. For example, different types of complements to self assessment might be more appropriate for large utilities than for small utilities.

The WSWG considered only a voluntary national aggregate measures effort. The Group acknowledges that a purely voluntary effort will face challenges to providing a complete and accurate picture of sector progress. At the same time, the WSWG identified a number of factors that should prompt utilities to participate in a voluntary national aggregate measure effort including:

› Credible voluntary measurement efforts will increase the overall credibility of the sector; and
› A defined measurement effort to evaluate security needs and progress will build national support for security efforts and funding by demonstrating need.

Finally, the WSWG acknowledges the difficulty, in general, of establishing a measurement system for programs, like security, that are preventive in nature. The Group recognizes that an important objective of security enhancement is to increase the competency and capabilities of local officials (for example, through community training and exercises), something that may not be indicated through measures of activities. As discussed earlier in this document, the Group encourages consideration of movement towards measures that are more oriented to security outcomes over time.

Progress Implementing Active and Effective Security Programs

For a potential measure of implementation progress, the WSWG suggests: *Amount and degree of implementation of the 14 features of an active and effective security program.*

Earlier in this document (see Finding 5, feature 14), the WSWG identifies the features of an active and effective security program, and suggests that utilities carry out self assessment of their progress towards implementing active and effective security programs. The WSWG also suggests a specific set of measures that tie to each of the program features (see Finding 16) and suggests that at least once per year, utilities carry out a self-assessment to evaluate their security practices and progress (see Finding 5, feature 14). These self assessments could provide for a national aggregate picture of the degree of implementation of each of the 14 features of an active and effective security program.

Utilities would assess their degree of implementation of each of the 14 features, based on evaluation of the feature-related measures, using a "high, medium, low" scale. A "high" rating would indicate a utility has fully addressed a program feature; a "medium" rating would indicate a utility is in the process of addressing a program feature (i.e., it has begun but not completed work); and a "low" rating would indicate a utility has not begun, or cannot yet begin, to address a program feature. The Group also discussed this as a stoplight concept, where fully addressed program features are green, features that are in progress are yellow, and features not yet begun are red.

This measure will provide a sense of the number and percent of utilities fully addressing each feature of an active and effective security program, and the number and percent of utilities making progress towards fully addressing all program features. Examining progress on a feature-by-feature basis, using the feature-related measures, should indicate where additional attention is needed—features for which progress is limited or lacking across the sector may benefit from additional assistance or guidelines.

The WSWG initially considered this measure in a substantially simpler form, where utilities would use a simple yes or no to indicate whether they had addressed each feature of an active and effective security program. Many of the measures suggested for utilities to consider in Appendix C and some of the measures suggested for utilities to use in Appendix A take a binary approach. The WSWG ultimately rejected a binary approach for national, aggregate measures, because such an approach would not recognize efforts already underway and would likely misrepresent the water sector's progress. The WSWG anticipates that many utilities will address the 14 features over several years, making more or less progress in each area, depending on utility-specific circumstances and operating conditions. The suggested high/medium/low approach is designed to provide a more nuanced sense of utility security progress.

Progress Reducing the Number of Security Risks

For a potential measure of progress reducing the number of security risks, the WSWG suggests: *Total number of assets determined to be a high security risk and the number of former high-security risk assets lowered to medium or low risk, based on assessments of vulnerabilities.*

Under the Bioterrorism Act, community water systems serving over 3,300 people are required to assess system vulnerabilities. Earlier in this document (see Finding 5, feature 3), the WSWG suggested that all utilities (including utilities serving 3,300 or fewer people that were not addressed by the Bioterrorism Act) maintain an assessment of vulnerabilities as a living document. Utilities have a number of standard publicly or commercially available vulnerability assessment methodologies available to them. Each of these methodologies approaches the assessment of vulnerabilities somewhat differently and produces slightly different reports. Some methodologies, such as the RAM-W or VSAT methodologies, translate qualitative risk assumptions into somewhat quantitative vulnerability reports. Other methodologies, such as the SEMS methodology, produce more narrative reports or checklists, and have been used by many smaller utilities.

Regardless of the methodology used, one of the outcomes of any robust assessment of vulnerabilities is a sense of utility-specific assets that present a high risk from a security standpoint (i.e., a set of assets determined to be a high security risk, or, a set of high-risk security assets). For example, the SEMS methodology provides an inventory of utility assets and assigns a high, medium, or low ranking to each. Identification of high-risk assets considers both vulnerability to threats and the potential consequences of an event, and assets can move from high to medium or low risk based on either reduction in vulnerabilities or mitigation of potential consequences. In all of the methodologies, identification of assets that constitute a high risk from a security standpoint considers both vulnerability to threats and the potential consequences of an event; assets can move from high risk to medium or low risk based on either reduction in vulnerabilities or mitigation of potential consequences.

This measure would track, on a snapshot basis, the total aggregated number of high-risk assets identified and the number of high-risk assets that are reduced to lower risk status over time. This change in risk status, from high to medium or low, represents progress of the sector in addressing high-risk assets by, for example, protecting against vulnerabilities or taking steps to mitigate potential consequences. It is consistent with discussions of sector-related measures in the National Infrastructure Protection Plan, where EPA and DHS are discussing measurement of assets reduced from high to lower risk.

In their deliberations on a measure of progress in reducing security-related risk, including reductions in the number of high risk assets, the WSWG discussed issues associated with the baseline against which progress would be measured. The Group acknowledges that an initial baseline must be established and that this baseline may change over time as utilities update their vulnerability assessments. For example, if a utility changes its design basis threat assumptions, this may result in a change to the utility's baseline list of high-risk assets. Provided basic threat and operating conditions do not change, a utility should expect the total number of high-risk assets to decrease over time, as security improves. Of course, the number of high-risk assets also might increase over time as a result of increased attention to security or lessons learned from exercises and actual event responses. The WSWG emphasizes that the number of high-risk assets will, in all cases, be simply a snapshot of the current state of the sector.

The Group recognizes that the Bioterrorism Act applies only to larger systems, and that some smaller systems may not yet have completed vulnerability assessments. This will be an important consideration in structuring the details of this progress measure. For example, it may be that the baseline of total high-risk security assets present in the water sector will appear to go up in initial years as smaller systems complete vulnerability

assessments and put active and effective security programs in place, even though, in fact, these actions on the part of smaller systems likely are increasing the overall security of the sector.

Progress Reducing the Risk Potential Inherent in Utility Operations

For a potential aggregate measure of progress reducing the risk potential inherent in utility operations, the WSWG suggests: *Potentially effected residential population inside the Clean Air Act Section 112(r) worst-case scenario off-site consequence analysis areas of water and wastewater utilities nationwide, and number of utilities that have converted from gaseous to other forms of chlorine or other treatment methods*.

Under Section 112(r) of the Clean Air Act, facilities at which certain types of extremely hazardous substances are stored or used must carry out modeling and other analysis to determine the potential effects of a sudden, catastrophic air release of these substances, and to determine the potentially effected population. In 2004, approximately 1,800 drinking water and 1,200 wastewater utilities reported the results of internal assessments of potential chemical release impacts, due largely to use of gaseous chlorine, anhydrous ammonia, aqueous ammonia, and anhydrous sulfur dioxide. This measure would draw only on these already-reported data to evaluate progress in reducing the potential worst case consequences of a successful attack on chemical storage at water and wastewater utilities.

EPA also should consider how data on the largest single vessel of Clean Air Act 112(r) hazardous substances maintained on site and the end-point distance of the worst-case scenario might create a more complete picture of utility efforts to reduce the consequences of a successful attack on chemical storage at a utility. Each of these data sets is already part of Section 112(r) reporting. By considering these data, measures might more fully recognize water sector efforts in increasing protection of the public through, for example, reducing the number and size of containers or implementing passive release containment or mitigation measures or similar safeguards. Because Section 112(r) allows for consideration of administrative controls that limit the maximum quantity of hazardous substances held in a single vessel and passive mitigation systems, consideration of these data also would acknowledge some utility efforts to increase the safety of on-site chemical storage. (Passive mitigation systems are systems that operate without human, mechanical, or other energy input and include building enclosures, dikes, and containment walls.) The WSWG notes that the mitigation measures that are considered under Section 112(r) represent only a few elements of active and effective security programs contemplated by the WSWG. As a complement to this measure based on Section 112(r) data, measures related to implementation of active and effective security programs provide for consideration of the full range of mitigation efforts utilities might undertake.

The WSWG notes a number of very important caveats to Section 112(r) data that should be provided as context for any use of this national aggregate measure. Most importantly, utilities do not control the number of people who choose to live near their infrastructure and, therefore, can only control the size of their off-site consequence analysis area, not the number of people who live in the off-site consequence analysis area. Utilities might undertake aggressive hazardous substance reduction efforts that are masked, at least in part, by population infill which they do not control. In addition, efforts to reduce the inherent hazards associated with water and wastewater treatment cannot be simplified to a finding that would call for the total elimination of the use of hazardous substances. For example, in the drinking water industry, residual chlorine is required in the distribution system. The WSWG emphasizes that decisions about how to manage the risks associated with use of hazardous substances are complicated. For example, reductions in the size of hazardous substance containers have the potential to reduce the size of the off-site consequence analysis area and reduce the number of people who could be at risk during a catastrophic release. At the same time, smaller containers mean more

frequent delivery of substance, and more transportation of these substances over roads and through communities.

As a supplement to measurements that rely on data already reported under the Clean Air Act Section 112(r), EPA also should measure the number or percentage of utilities that have converted from gaseous chlorine to liquid or solid form chlorine or other water treatment methods such as ozone or ultra-violet light. A measure of conversion from gaseous chlorine would supplement consideration of Clean Air Act Section 112(r) data by providing important detail on steps utilities are actually taking (and actions utilities can control) to reduce the risk potential of utility operations.

Other Measures Considered

The WSWG considered, but ultimately decided not to suggest, a national, sector wide, aggregate measure of progress related to improvement in utility contaminant detection efforts. Earlier in this document (see Finding 5, feature 7), the WSWG called on utilities to employ protocols for detection of contamination consistent with the recognized limitations in current contaminant monitoring technologies. The Group also recognized and expressed concern that utilities' abilities to undertake chemical, biological, and radiological monitoring of contamination are limited, in large part, by the lack of reliable or affordable technology and the lack of guidance or experience with how to interpret monitoring results. (See Finding 8.) At the same time, the Group is keenly interested in rapid development of practical contaminant detection approaches and in improving contaminant detection in the water sector, and was interested in the role a national, sector wide, aggregate measure of progress in contamination detection could play in creating pressure on EPA and other government agencies to promote and support rapid development of practical contaminant detection approaches.

Because current limitations in contaminant detection technologies create a barrier to meaningful measurement of progress, ultimately, the WSWG decided to place a national, sector wide, aggregate measure related to contaminant detection in a "wait and see" category. The Group reiterates its concern that utilities' abilities to undertake chemical, biological, and radiological monitoring of contamination are limited, in large part, by the lack of reliable or affordable technology and the lack of guidance or experience in how to interpret monitoring results, and again strongly encourages government to continue and increase financial and other support for the development of chemical, biological, and radiological monitoring technologies, and to assist utilities in creating protocols and guidance for interpretation of contaminant monitoring data. As progress in developing practical contaminant detection approaches is made, the Group encourages EPA and other government agencies to continue to explore a national, sector wide, aggregate measure of contaminant detection performance.

Reporting

The WSWG is not making a specific finding on reporting methods or frequency for national, sector wide, aggregate measures. To the extent EPA determines national reporting is needed, the Agency should address reporting methodologies and frequencies in collaboration with the water sector and water sector stakeholders at that time.

APPENDIX A: FEATURES AND MEASURES OF AN ACTIVE AND EFFECTIVE SECURITY PROGRAM

In Finding 5, the WSWG identified 14 features of active and effective security programs to provide for consistency in security outcomes across utilities, to guide utilities' consideration and selection of specific security approaches and tactics, and to create a foundation from which improvements in security can, over time, be measured and described.

The 14 program features define high-level security program outcomes, rather than specific security approaches or tactics. They were selected from among many potential features of security programs as those that, in the experience and view of the WSWG, are most important to increasing security and most relevant across the broad range of utility circumstances and operating conditions. The features are broadly drawn to allow individual utilities to tailor security approaches and tactics to utility-specific circumstances and operating conditions. At the same time, they are sufficiently important and relevant that they apply across the full range of utility conditions and should be addressed by all utilities. The WSWG emphasizes that significant variability in implementation of the program features is to be expected and is appropriate; however, to have an active and effective security program, utilities should address each feature and develop specific implementation approaches and tactics tailored to their circumstances.

In Finding 16, the WSWG identified security program measures that relate to each feature. Like the program features, these measures are sufficiently broad to apply across the range of utility circumstances and operating conditions, and sufficiently important that they are suggested for all utilities as the basis of a utility-specific security measurement program.

Appendix A is designed to bring together the 14 program features identified in Finding 5 and the program measures defined for each program feature in Finding 16. Each feature and measure is described in detail below.

Explicit Commitment to Security

Feature 1—Water and wastewater utilities should make an explicit and visible commitment of the senior leadership to security.

Active and effective security programs do not exist in a vacuum—they are integral parts of the organizations they serve. To reinforce this idea, utilities should create an explicit, visible, easily communicated, enterprise-wide commitment to security.

Many water and wastewater utilities might make an explicit and visible commitment to security by incorporating security into a utility-wide mission or vision statement. Mission or vision statements, if used, should be simple, but complete. They should address the full scope of an active and effective security program—that is, protection of public health, public safety, and public confidence. They also should place security in the context of water and wastewater utilities' overall core operations, and recognize utilities' commitments to serving the public trust.

As with any enterprise-wide commitment, the process of development of an explicit and visible commitment to security may be just as important as the actual language of the statement that emerges from the process. Utilities should use this process as an opportunity to raise awareness of security throughout the organization and to help every facet of the enterprise to recognize the contribution they can make to enhancing security.

Utilities also might make an explicit and visible commitment by promulgating an enterprise-wide security policy, or set of policies. If used, these policies, like a mission or vision statement, should address the full scope of an active and effective security program and should be developed using a process that raises awareness of security throughout the organization.

No matter the approach used, the important outcomes are that the utility makes an explicit commitment to incorporating security into day-to-day operations and that this commitment is visible to all employees and customers.

Measure 1—Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?

As discussed earlier in this document, to be successful, active and effective security programs cannot exist in a vacuum—they should be integral parts of the organizations they serve. This measure establishes the expectation that, as part of their self assessment and measurement efforts, utilities will ask themselves whether they have an enterprise-wide security policy and whether the policy is being appropriately maintained. Note that this measure contemplates that, as part of an active and effective security program, a utility will develop a written, enterprise-wide security policy, establish a schedule for regular review of the policy, and update the policy as needed. The Group debated whether it is necessary for an enterprise-wide policy on security to be written and ultimately determined that written policies are needed to help make a utility's commitment to security visible and tangible throughout the organization. The Group has chosen not to specify a timeframe for what constitutes "regular" review of an enterprise-wide security policy; utilities should establish timeframes appropriate to their specific circumstances and operating conditions. Many WSWG members believe review of an enterprise-wide security policy should be carried out at least once every year, as part of a yearly review of security performance, and that yearly security reviews should be incorporated into yearly enterprise-wide planning and budgeting activities. Integrating security into wider organization planning and budgeting in this way has the potential to highlight instances where a security improvement may also create operational improvement (or vice versa), and will reinforce security as part of the overall organization culture.

Security Culture

Feature 2—Water and wastewater utilities should promote security awareness throughout their organizations.

Every person in a utility organization has something to contribute to enhancing security and every person should be expected to make a contribution. The objective of a security culture should be to increase security by making security awareness a normal, accepted, and routine part of day-to-day operations. The importance of a security culture cannot be overstated. The best security plans and procedures in the world will not work if they are not implemented—and implementation relies on line staff and managers. Workers on the front lines of an organization are the people most likely to have occasion to notice something out of the ordinary that may signal a threat to security. Attentiveness on the parts of these individuals, and willingness to bring potential security

issues to the attention of others, is something a utility can implement to improve security regardless of size or location.

Creating a security culture involves efforts that are easily described and very tangible, and efforts that are less easy to describe and less tangible. Examples of tangible efforts include: employee training; incorporating security into job descriptions, performance standards, and evaluations; creating and maintaining a security tip line and suggestion box for employees; making security a routine part of staff meetings and organization planning; making security visible in day-to-day operations through use of badges and signs; and creating and implementing measures of security activities and progress.

Some utilities have created a security management team or oversight committee; a group of department heads and other leaders in the organization that meets regularly to establish security procedures, set security priorities, and ensure cross-organization coordination. A security oversight committee creates a solid, lasting foundation on which a security program and security culture can be built. At some utilities, the security oversight committee is also responsible for responding in real-time to threats and security events. This combination of oversight and response duties keeps security policy connected to the practical side of security implementation.

Less tangible efforts to instill a culture of security throughout an organization are fully as important as the more tangible efforts, but are difficult to describe. In general, they have to do with those in positions of authority in an organization rewarding attentiveness to security, creating a culture where reporting of problems or suspicious events is the norm, and leading by example. For example, those in leadership positions might make a point of following security procedures visibly; if badges are required, they would wear security badges. Employees who raise security concerns and who demonstrate attentiveness to security would be acknowledged and rewarded, and awareness programs would give employees timely and useful information about current threats and what to look for. All employees would be given an opportunity to contribute to security, not just by wearing identification and following procedures, but also by reporting suspicious or threatening events and making suggestions for furthering security improvements, for which they would receive timely acknowledgement or feedback to reinforce the value of reports and suggestions.

Measure 2—Are incidents reported in a timely way, and are lessons learned from incident responses and training reviewed and, as appropriate, incorporated into future utility security efforts?

Feature 2 establishes the expectation that as part of an active and effective security program, a utility will promote security awareness throughout its organization. This measure highlights a key element of security awareness—the ability of an organization to quickly identify security incidents and to incorporate lessons learned into future security efforts. As part of implementing this measure, the WSWG believes utilities should pay particular attention to circumstances, if any, where it becomes clear that a security incident was not reported in a timely way. This might be the case, for example, where employees are aware a lock or other security barrier is damaged, but do not report it, so the damage is instead discovered by an internal utility audit or other security check. These circumstances are important indications of the extent to which security tactics and approaches are working on the "front lines" of an organization and are a key measure of the presence (or absence) of a security culture. Measure 2 also suggests utilities explicitly review responses to security incidents and incorporate lessons learned into future security efforts, as appropriate. This ongoing learning and adapting as utilities gain experience with security is key to increasing the protectiveness of a security program and to creating a security culture. Note that the Group chose not to establish a standard timeframe for what constitutes "timely" reporting of incidents. Instead, utilities should establish incident reporting expectations appropriate to their specific circumstances and operating conditions.

Up-to-Date Assessment of Vulnerability

Feature 3—Water and wastewater utilities should assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.

Understanding and assessment of vulnerabilities is a key building block of an active and effective security program. It establishes critical security needs, identifies and describes utility-specific circumstances and operating conditions that define vulnerability, and establishes the key risks and security enhancement priorities that will drive security planning. Over time, utilities should expect that the conditions that defined their initial assessments of vulnerability will change—they may become less vulnerable because of changes to circumstances, infrastructure, or operating conditions, or they may become more vulnerable because of changing threat or attack probabilities. Threats will change over time and security improvements will change a utility's susceptibility to ongoing and new threats. Because circumstances change, utilities should continually adjust their security enhancement and maintenance priorities so they remain responsive to vulnerabilities.

This finding establishes the expectation that utilities should maintain their understanding and assessment of vulnerabilities as a "living document" that reflects current security-related conditions. To accomplish this objective, utilities should periodically review and update their assessment of vulnerabilities and risks, including the design basis threat used as the foundation of the vulnerability assessment. The timing for review will vary across utilities, depending on the degree to which security-related conditions are changing and resources are available. Utilities should consider their individual circumstances and establish and implement a schedule for review of their vulnerabilities. At a minimum, the WSWG believes all utilities should reassess their vulnerabilities and risks at least once every three to five years. Conditions that might prompt more frequent review of vulnerabilities include major facility construction projects, adding new facility infrastructure (by construction or acquisition), new information about specific threats, and significant attacks or other events that would cause reconsideration of utility vulnerability. Many WSWG members believe utilities would be well served by reviewing their assessments of vulnerability annually, and believe an annual review should take place. For these updates to assessments of vulnerabilities to be carried out, it also is important for EPA and DHS to provide updated, timely, actionable threat information to the water sector. As discussed more fully in feature 10, more progress is needed in this area.

Reviews of vulnerabilities should be carried out by those involved in the security program and knowledgeable of utility operations. An executive should be included to provide an ongoing conduit of information to and from management, and so that management's awareness of security continues to grow. The information considered during the review and any changes to the understanding or assessment of vulnerabilities should be documented, so utilities can form a long-term basis for decision making and track their progress over time.

The WSWG notes that there are a number of publicly or commercially available methodologies utilities can use to help them understand and assess vulnerabilities, and new methodologies are being developed. These methodologies may be very helpful to utilities in that they create a standard process for vulnerability assessment that can be replicated, so changes in vulnerability can be measured over time. The WSWG is not suggesting use of any particular vulnerability assessment methodology. Rather, utilities should use the methodology that best suits their particular circumstances, taking care to ensure consideration of the significant system failures and key threats or methods of attack suggested for consideration earlier in this document (see Finding 3). EPA has published guidance on the basic elements of sound vulnerability assessments; these elements are:

- Characterization of the water system, including its mission and objectives;
- Identification and prioritization of adverse consequences to avoid;

- Determination of critical assets that might be subject to malevolent acts that could result in undesired consequences;
- Assessment of the likelihood (qualitative probability) of such malevolent acts from adversaries;
- Evaluation of existing countermeasures; and
- Analysis of current risk and development of a prioritized plan for risk reduction.

Measure 3—Are reassessments of vulnerabilities made after incidents, and are lessons learned and other relevant information incorporated into security practices?

Feature 3 establishes the expectation that utilities should maintain their assessments of vulnerabilities as living documents that reflect current threats and utility-specific security tactics and approaches. This measure suggests that utilities reassess vulnerabilities after incidents, and incorporate lessons learned and other relevant information into security practices. For example, lessons learned in reassessing vulnerabilities after incidents might help a utility improve its practices for access detection and control. Alternatively, lessons learned might help a utility identify new security priorities and change the way it invests security resources. As discussed throughout this document, the WSWG believes strongly in the importance of ongoing, thoughtful reassessment and adaptation, as a way to keep security programs "fresh" and effective, take advantage of emerging approaches and new technologies, and perpetuate a security culture throughout an organization.

Resources Dedicated to Security and Security Implementation Priorities

Feature 4—Water and wastewater utilities should identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.

No organization can sustain focus on a priority in the absence of dedicated resources, and utility security is no different. To ensure utilities sustain focus on their ongoing security programs and on security improvement priorities, this feature establishes the expectation that utilities should, through their annual capital, operations and maintenance, and staff resources plans, identify and set aside resources consistent with their specific identified security needs.

The WSWG highlights three ways that utilities might invest resources in security.

First, and perhaps most importantly, utilities can and should "invest" in security by increasing the amount of time and attention that executive and line managers give to security. It is important not to underestimate the value of these contributions—just increasing attentiveness will improve security, even if no other changes or investments are made. Utilities might ensure this extra attentiveness by including security in semi-annual performance reviews and progress reports, or by making security a standing item on executive management agendas.

Second, utilities will invest staff time and resources in security by including security considerations in budgets for personnel and training. For some larger utilities, this might include adding new staff dedicated to security. For others, particularly smaller utilities, it may mean specific acknowledgment that existing staff are taking on new security-related responsibilities. In both cases, utilities should account and plan for the staff costs associated with security responsibilities. Utilities also might dedicate resources to security by including security training and exercises in their annual operations plans. Even when training and exercises are absorbed by regular operating budget categories, it should be acknowledged that these expenses will occur, and that covering these security-related expenses may represent a decision to do less of something else.

Third, and perhaps most obviously, many utilities will make ongoing capital investments in security. Capital investments might include physical hardening of structures, investment in monitoring devices, purchase of emergency response equipment, and design and construction of new facilities and infrastructure.

The WSWG recognizes that utilities always must balance resource allocations among a number of important obligations. To reflect their ongoing commitment to security and to, over time, balance resource allocations among security improvements and other organizational priorities, utilities should establish clear security improvement priorities.

One way that utilities might record their security improvement priorities is in a security improvement plan. Security improvement plans create a clear sense of security priorities and place those priorities in the context of other organizational priorities. Successful security improvement plans address what a water or wastewater utility will do relative to all features of an active and effective security program; not only those associated with physical hardening or access control, or those that require significant capital investment. For example, a successful security improvement plan will address activities that help to build a security culture in an organization and activities associated with building community partnerships, just as much as it addresses investments an organization will make in new equipment to improve security.

Whatever means utilities use to document their security improvement priorities, these priorities should be clearly recorded in a living document that will, by definition, change over time. Security improvement priorities should be reviewed, along with other annual plans and investments, with top utility executives at least once a year. This review might include an update/status report on security enhancements undertaken to date, a high-level review of remaining vulnerabilities and risks, and a description/identification of priorities for the upcoming and future years. Over time, this type of annual review will give utilities the information they need to carry out trend analysis, document progress, and form opinions on whether the level of resource investment in security is appropriate.

To the extent appropriate, utilities might integrate a security improvement plan with other annual operating plans. Such integration may provide a valuable opportunity for utilities to continue to integrate security into day-to-day management, operations, and tracking. It also may serve to highlight areas where a potential security improvement would also create value for another part of the organization; for example, where a monitoring protocol that improves security also improves operations, by allowing operators to fine-tune treatment systems more efficiently and effectively. In general, the WSWG believes that utilities are best served by incorporating security considerations into the enterprise-wide capital and operating budgets and plans that are already prepared.

It is important to note that the WSWG is not suggesting a standard dollar amount of security investment that would be appropriate for all utilities. As discussed earlier in this document (see Finding 1), each individual utility must tailor their security approaches and tactics to their specific circumstances. For some utilities, it may be necessary and practical to make large capital investments in security, or to invest in dedicated security staff. For other utilities, especially smaller utilities, the potential for capital investment may be much less—and much less needed—and new security-related responsibilities and attentiveness will be absorbed into existing staff responsibilities. The key is that utilities make some investment and that whatever the level of investment of a particular utility, the investment is made consciously and in light of a thoughtful assessment of vulnerabilities and related security improvement priorities.

Measure 4—Are security priorities clearly identified, and to what extent do security priorities have resources assigned to them?

Some WSWG members believe informed identification of security priorities and corresponding resource decisions are the keys to an active and effective security program. Feature 4 establishes the expectation that utilities will identify and set aside resources consistent with their specific identified security needs in their annual capital, operations, and maintenance budgets, and staff resources plans. This measure establishes the expectation that utilities will monitor the extent to which priorities are identified and resourced. Note that the WSWG does not assume all security priorities will have resources assigned to them. The Group recognizes that utilities may have security priorities in which they cannot afford to invest. This measure reflects the Group's belief in the importance of utilities recognizing and monitoring these situations, and understanding utilities' ability to invest in security over time.

Defined Security Roles and Employee Expectations

Feature 5—Water and wastewater utilities should identify managers and employees who are responsible for security, and establish security expectations for all staff.

While all utility employees likely have a contribution to make to security, establishing overall responsibility for ensuring a utility's security plans are implemented and maintained is important to creating a sense of accountability for security and providing for security-related leadership. Explicit identification of security responsibilities also is important for development of a security culture. Accountability for security should be clearly fixed with an individual or individuals, and established at a high enough level to ensure that security is given management attention and to make security a priority for line supervisors and staff.

WSWG members defined a number of crucial security-related roles and responsibilities utilities might consider, including security program implementation management, physical intrusion and contamination detection, and incident command roles during emergency response and recovery. At a minimum, utilities should identify a single, designated individual responsible for overall security, even if other security roles and responsibilities will likely be dispersed throughout the organization. In addition, security expectations should be included in job descriptions and annual performance reviews for all employees with security responsibilities. Even when security is not a full-time duty, there should be an assigned manager in the utility who is responsible for operating a meaningful security program.

The WSWG emphasizes that implementation of this finding will differ, potentially substantially, depending on a utility's specific circumstances. For example, large urban utilities might create a security department with a director and staff fully dedicated to security program implementation. Alternatively, a small rural utility might assign all security program implementation responsibilities as part of one individual's job.

Measure 5—Are managers and employees who are responsible for security identified?

Feature 5 reflects the WSWG belief that accountability for security should be clearly fixed with an individual or individuals, and established at a high enough level within the organization to ensure security is given management attention and to make security a priority for line supervisors and staff. This measure suggests that utilities should assess whether they have clearly fixed responsibility for security by evaluating whether they have identified managers and employees with security responsibilities. As described earlier in this document, it is important to recognize that the WSWG is not suggesting a specific security staffing or management structure. Large urban utilities may create a security department with a director and staff. Smaller utilities may assign all

security responsibilities to an existing employee or to a general manager. Both approaches are consistent with the WSWG's finding, provided the responsibility for security is clearly understood and there is accountability for security with organization leadership.

Access Control and Intrusion Detection

Feature 6—Water and wastewater utilities should establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business, and to detect unauthorized physical intrusions.

Intrusion detection and access control is a cornerstone of all active and effective security programs. Utilities should implement measures to deter unauthorized intrusions to facilities and operations, and to detect unauthorized access to utility assets in a manner that is timely and enables the utility to respond effectively.

Access control will involve both physical and procedural means to restrict access to treatment facilities and to supply/distribution/collection networks, for the purposes of deterring physical harm and/or the introduction of harmful chemical, biological, or other substances into the water supply/treatment/distribution and wastewater collection/treatment systems. Examples of physical access controls include fencing critical areas, locking gates and doors, installing barriers at site access points, and installing tamperproof devices at key distribution points. Procedural examples include inventorying keys, changing access codes regularly, requiring security passes to pass gates and access sensitive areas, establishing a security presence at facility gates, requiring all visitors to have scheduled appointments, requiring visitors to sign in at a front desk and display identification at all times, implementing chemical delivery and testing procedures including chain of custody control, limiting delivery hours, and checking all deliveries to ascertain nature of material. The American Water Works Association Research Foundation's (AWWARF) *Security Practices Primer for Water Utilities* (2004) provides additional information on physical and procedural access controls.

Monitoring for physical intrusion can include such physical enhancements as maintaining well-lighted facility perimeters, monitoring with closed caption TV, installing motion detectors, and utilizing intrusion alarms. Procedurally, the use of neighborhood watches, regular employee rounds, and arrangements with local police and fire departments can support identifying unusual activity in the vicinity of facilities.

All employees, including contractors and temporary workers with unescorted access to facilities, should have their identity verified through background checks to reduce the possibility that ill-intentioned individuals are present in an organization. The degree and rigor of background checks can be tailored to the responsibilities and privileges of the employee, and utility-specific circumstances and operating conditions. For example, front office clerical staff with no access to critical facility operations might receive a lower level of screening than plant operators. In small communities, utility officials might have first hand knowledge of an individual's background, which could act as an effective screening method absent a more formal background check. Adjusting the degree and rigor of background checks to specific circumstances will help utilities manage concerns related to the costs of checks and checking delays.

WSWG members believe effective background checks are a very useful way to verify employee identity, establish citizenship, previous criminal activity, and work eligibility, and to confirm the individual is not on a current terrorist watch list. Group members support using background checks for these purposes, even as they recognize that some publicly-funded utilities may face legal barriers or constraints on their ability to use

background checks, particularly for existing employees. The Group encourages public agencies to work to overcome these barriers so that they can use background checks to enhance security.

While background checks represent a sound business practice and can deter ill intentioned people from attempting to establish employment, it is important to understand that they are just one part of an effective intrusion detection and access control program. Background checks may not be sufficient to identify or deter a determined, sophisticated, systematic attempt to infiltrate a utility organization, since in these cases, individuals with passable backgrounds are likely to be used. In addition, background checks might create impediments to business if requirements are overly broad such as to restrict appropriate site access for emergency responders, customers, business visitors, union industrial hygienists, and others, and should not create overly burdensome cost barriers to legitimate access to employment or information.

Utilities also should establish the means to readily identify all employees. Many utilities find that use of identification badges or other photo identification is an efficient way to identify employees. Photo identification badges can be displayed by all employees at all times, in plain sight. For some utilities, it has been helpful to tie identification badges into systems of access control, allowing only certain employees access to security-sensitive or other critical areas; these systems also can be used to quickly deny access to any individual in the event of an emergency or a security-related concern.

The WSWG notes that individual utilities may choose to place more or less emphasis on access control versus intrusion detection. For example, some small utilities have recognized that, as a practical matter, it may be very difficult to control access to remote, unguarded infrastructure, and have chosen to invest more heavily in systems or procedures that detect unauthorized access (intrusion) and enable the utility to respond appropriately.

Measure 6—To what extent are methods to control access to sensitive assets in place?

Feature 6 calls on utilities to establish physical and procedural controls to detect unauthorized intrusions and restrict access to utility infrastructure to only those conducting authorized, official business. Measure 6 highlights a key subset of efforts to detect intrusions and control access by focusing on sensitive assets. The Group is not describing a standard list of sensitive utility assets, or a particular set of approaches or tactics that should be used to detect and control access. Rather, utilities should identify sensitive assets based on their specific circumstances and operating conditions, and should develop and implement utility-specific access control approaches and tactics. There are a number of ways that utilities might assess the "extent" to which methods to detect intrusions and control access are in place. For example, utilities just beginning to develop a security program might measure the number and percent of sensitive assets protected by access control methods. Utilities with more experience might test intrusion detection and access control methods at sensitive assets and measure their performance. Over time, measure 6 contemplates that utilities will have well functioning intrusion detection and access control methods in place for all sensitive assets.

Contamination Detection, Monitoring, and Surveillance

Feature 7—Water and wastewater utilities should employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.

Contamination detection, contaminant monitoring, and surveillance are different but related elements of a contamination warning system. The WSWG discussed three points with respect to contamination detection,

monitoring, and surveillance: physical monitoring or surveillance for contaminants; monitoring or surveillance of indicators of contamination; and connections with customers and public health providers.

Physical monitoring or surveillance for chemical, biological, and radiological contamination is an evolving area, with research underway to provide for more direct and real time methods. Currently, physical monitoring and surveillance for contamination is limited in large part by a lack of reliable or affordable technology and the lack of guidance or experience in how to interpret monitoring or surveillance results. In Finding 8, the WSWG addresses the need to support development of practical, real-time contaminant monitoring and surveillance systems and protocols to help utilities evaluate and respond to contaminant monitoring and surveillance data. With a grant from EPA, the American Society of Civil Engineers recently issued *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*. These guidelines provide information on assessing the need for a contaminant monitoring system, locating instruments and sensors, and responding to suspected contamination events.

While encouraging use of online contaminant monitoring or surveillance systems where they can be put into place, the WSWG also recognizes that much of the basic scientific and engineering knowledge needed, and the instrumentation needed to accomplish the job directly, is not yet available in the marketplace. Other guidelines, such as AWWARF's *Design of Early Warning and Predictive Source-Water Monitoring Systems* (2001) and *Online Monitoring for Drinking Water Utilities* (2002), and EPA's Response Protocol Toolbox, also encourage use of current contaminant monitoring approaches, while recognizing the limitations of current approaches and the need for additional research and development. Until progress can be made in development of practical and affordable online contaminant monitoring and surveillance systems, most utilities must use other approaches to contaminant monitoring and surveillance.

In the absence of practical technologies for contaminant monitoring and surveillance, routinely monitored physical and chemical parameters hold some potential to act as contamination surrogates (signaling possible contamination problems), but this potential is limited. Until new technologies are reliable and affordable, some utilities are trying to use careful monitoring of physical and chemical contamination surrogates, and use surrogate data, as an indicator of possible contamination problems. Physical and chemical contamination surrogates include pressure change abnormalities, free and total chlorine residual, heterotrophic plate count, high volume total fecal coliform analysis, temperature, dissolved oxygen, conductivity, oxygen-reduction potential, total dissolved solids, turbidity, pH, color, odor, and taste.

Many utilities already measure these parameters on a regular basis to control plant operations and confirm water quality; more closely monitoring these parameters may create operational benefits for utilities that extend far beyond security. For example, by more closely monitoring water quality parameters, one utility was able to more effectively target chlorination, thereby reducing operating costs and chlorine usage. At the same time, there are limited data and experience correlating changes in routinely collected physical or chemical monitoring data with actual contamination events. Often, the relevance of changes in these data to security can be difficult to interpret and, therefore, is difficult for utilities to act upon from a security perspective.

Finally, utilities also should thoughtfully monitor customer complaints and improve connections with local public health networks to detect public health anomalies. While the WSWG emphasizes that using customers as indicators of potential contamination problems is far less than ideal, at a practical level, until contaminant monitoring technologies are improved, attention to customer complaints and public health anomalies are an important way to detect potential contamination problems and other water quality concerns. Utilities should consider customer complaints from a security-related perspective and should forge closer connections and partnerships with their local public health communities, so that public health anomalies can be evaluated for

water security implications. (The need to strengthen connections with public health also is addressed in Finding 7.)

Measure 7—Is there a protocol/procedure in place to identify and respond to suspected contamination events?

Feature 7 calls on utilities to employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection technologies. As discussed earlier in this document, the WSWG recognizes and is concerned that utilities' abilities to undertake chemical, biological, and radiological monitoring of contamination are limited, in large part, by the lack of reliable or affordable technology and the lack of guidance or experience in how to interpret monitoring results. Earlier findings call for aggressive financial and technical support for development of cost-effective, reliable contamination monitoring devices. At the same time, the WSWG believes that, as part of an active and effective security program, utilities should employ protocols for detection of contamination consistent with current recognized limitations. Efforts might begin with a close monitoring of routine water quality testing for anomalies that could signal a contamination event, monitoring public health anomalies and customer complaints, and having a protocol in place for responding to potential contamination events. Over time, contaminant detection efforts might be expanded to include periodic regular testing for contamination or event-based contamination testing (i.e., testing in the event of a specific threat, or identified security breach). In the future, practical, in-line, real-time parameter-specific contaminant detection approaches may become available.

Regardless of the approach to contaminant detection a utility uses, measure 7 highlights a crucial aspect of the success of contaminant detection: the existence of a protocol to identify and respond to suspected contamination events.

Information Protection and Continuity

Feature 8—Water and wastewater utilities should define security-sensitive information, establish physical and procedural controls to restrict access to security-sensitive information as appropriate, detect unauthorized access, and ensure information and communications systems will function during emergency response and recovery.

Information technology (IT) systems are critical to the smooth and consistent operation of water and wastewater utilities, and maintaining access to information and telecommunications systems during an emergency is critical to effective response. This feature establishes the expectation that utilities should protect IT systems, including SCADA systems; define and protect security-sensitive and vital information; and plan for effective communications during and after emergency responses.

With respect to protecting IT systems, the WSWG discussed two areas of emphasis: (1) restricting access to critical IT systems (such as SCADA) to authorized personnel conducting official utility business, and (2) maintenance of an uninterruptible power supply.

Protecting IT systems largely involves using physical hardening and procedural steps to limit the number of individuals authorized to access critical IT systems and to prevent access by unauthorized individuals. Procedural steps might include restricting remote access to data networks, safeguarding critical data through backups and storage in safe places, establishing procedures to restrict network access, and implementing policies to ensure that IT contractors and their products will not negatively affect IT systems. Examples of

physical steps to harden SCADA and IT networks include installing and maintaining firewalls, screening the network for viruses, separating business systems from operational systems, installing a system for virus protection, ensuring security and location of SCADA system components, encrypting access via modem to utility networks—including wireless networks, conducting regular penetration evaluations, avoiding connecting modems to desktop systems on the secure network, allowing remote access only from utility computers, and establishing and regularly changing computer system access codes.

Utilities should also strive for continuous operation of IT systems, even in the event of an attack, by providing for an uninterruptible power supply and the use of back up power generators or other back up power means.

It is also important to control access to security-sensitive information on utility operations or technical details that could aid terrorist planning and operations. The first step in this process is to review information sources to identify those containing security-sensitive information. This review will need to consider facility maps and blueprints, operations details, hazardous material utilization, tactical level security program details, and any other information on utility operations or technical details that could aid in planning or execution of an attack. Identification of security-sensitive information should consider all ways that utilities might use and make public information (e.g., many utilities may at times engage in competitive bidding processes for construction of new facilities or infrastructure). While there is an interest in ensuring that such bidding processes are in fact competitive, care also should be taken to safeguard security-sensitive information. Some utilities use bid pre-qualification systems to screen potential bidders for security purposes and then restrict access to security-sensitive information to screened bidders. Because many utilities are public or quasi-public agencies, and all utilities operate to serve the public trust, typically this review also will include developing an understanding of local freedom of information or Sunshine Act requirements to ensure access procedures fully comply with such requirements.

When security-sensitive information is identified, utilities should develop access restrictions and procedures to safeguard that information. At the same time, utilities should also develop procedures that make security-sensitive information available to employees and others who need it. If access restrictions are so severe as to limit practical use of information by employees, the restrictions likely will not be followed and security could be compromised. The WSWG is not suggesting a standard definition of security-sensitive information or a standard set of protocols to control access to such information. The water sector may wish to continue to work with federal agencies, and with community and public interest stakeholders, to create guidelines for identification of security-sensitive information and for providing appropriate access to such information. In the absence of such guidelines, utilities should develop protocols to identify and provide appropriate access to security-sensitive information, based on their specific circumstances and operating conditions.

In addition to controlling access to security sensitive information, utilities should take steps to ensure the preservation of information critical to the continuity of operations. These steps could include the identification of information needed to sustain day-to-day operations and arrangements for the back up and safe keeping of such information.

With respect to telecommunications, utilities should take steps to ensure the maintenance of critical internal and external communications in the event of an attack. In the event of an emergency, conventional telecommunications networks will come under severe pressure and may fail. Utilities should plan for this possibility and should evaluate the need and means for providing back up systems that will maintain contact with police, fire, and other first response organizations, and maintain internal communication with employees to ensure safety and to coordinate response activities.

Measure 8—Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how do control measures perform under testing?

Feature 8 calls on utilities to establish physical and procedural controls to define security-sensitive information, restrict access to such information as appropriate, and detect unauthorized access. Measure 8 suggests that utilities should assess whether they have the tools in place to define and restrict access to security-sensitive information, and evaluate their performance by reviewing whether information is correctly categorized and determining how access control methods perform under testing. Evaluating whether there is a procedure to identify and control security-sensitive information is straightforward. Evaluation of whether information is correctly categorized might take a number of forms, such as routine auditing or categorization tests. The purpose of evaluation of whether information is correctly categorized is to determine if a utility is identifying security-sensitive information in accordance with its utility-specific protocol, so that security-sensitive information is properly identified and controlled and, just as important, non-security-sensitive information is made available to the public as appropriate. Testing of access control methods might take a number of forms. For example, a utility might test paper document protection methods by submitting and then monitoring response to inappropriate document requests. Testing of electronic information protection methods might involve monitoring the performance of firewalls or other cyber protection devices. The WSWG is not suggesting specific testing protocols or frequency; instead, utilities should determine the testing that is most appropriate to their specific security tactics and approaches. The WSWG emphasizes that it does believe some testing of information access control measures is necessary to maintain an active and effective security program.

Design and Construction

Feature 9—Water and wastewater utilities should incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower risk design and technology options.

Over the long term, utilities have the opportunity to reduce their vulnerability and risk, in part by redefining the physical context in which they operate. This occurs as utilities make investments in new real estate or infrastructure, and repair and/or replace existing infrastructure. All such activities at utilities are guided by design and construction standards that direct and constrain the choices the organization will make. Utilities should incorporate security-related considerations into these standards, with the intent to reduce their inherent security risk over time.

To be effective, design and construction standards should address two dimensions of security risk: physical hardening of critical assets and the adoption of inherently lower security risk technologies and approaches. Physical hardening of critical assets is designed to deter and/or help mitigate physical damage, service disruption, or other serious consequences in the event of attack. Physical hardening involves designing-in the means to make a facility harder to attack (or appear harder to attack) and to reduce the effect of any attack that may take place. This typically involves considerations such as the location of critical infrastructure relative to perimeter areas and the natural shielding provided to infrastructure by the choice of building materials (e.g., concrete reinforced walls versus structural glass). Design choices also should consider the ability to ensure continuity of operations and rapid recovery in a successful attack, natural disaster, or other event.

The adoption of inherently lower security risk technologies and approaches involves considering how design and technology choices reduce the likelihood or extent of the consequences of concern. Such choices should further consider opportunities for reducing safety risk, in addition to security risk. For example, certain treatment

technologies may be less dependent upon the storage and utilization of hazardous chemicals, reducing both security and safety risks. Another example might be the purchase of additional buffer real estate, which can serve both to increase the stand-off and detection distance of a water supply or critical facility, and provide source water protection potential.

It is important to recognize that to incorporate security considerations into design choices, utilities need information about the types of security design approaches and equipment that are available and the performance of these designs and equipment in multiple dimensions. For example, utilities would want to evaluate not just the way that a particular design might contribute to security, but would also look at how that design would affect the efficiency of day-to-day plant operations and worker safety. Under a grant from EPA, AWWA recently issued *Interim Voluntary Security Guidelines for Water Utilities* (2004) and the Water Environment Federation recently issued *Interim Voluntary Security Guidance for Wastewater/Stormwater Utilities* (2004). These documents provide information for designers and owners/operators of water and wastewater utilities on design approaches and upgrades that improve security and reduce vulnerability. Other documents, such as the EPA Security Product Guides, provide information that can help utilities evaluate design options to optimize design choices.

Measure 9—Is there a protocol/procedure for incorporation of security considerations into internal utility design and construction standards for new facilities/infrastructure, and major maintenance projects?

As discussed earlier in this document, utilities have the opportunity to reduce their vulnerability and risk over the long term, in part by better incorporating security into utility design. Consistent with its principle of emphasizing prevention and encouraging use of inherently safer (i.e., lower risk) practices, the WSWG emphasizes the opportunity that design choices create to improve security. Feature 9 establishes the expectation that utilities will incorporate security considerations into decisions about acquisition, repair, and replacement of physical infrastructure, and will consider opportunities to reduce risk potential through physical hardening and the adoption of inherently lower risk design and technology options. This measure suggests that utilities verify they are bringing security considerations forward as early in the design process as practicable by incorporating security into internal utility design and construction standards, planning, and budgeting. Measure 9 also emphasizes the importance of considering security both during design and construction of new facilities, and during infrastructure and major maintenance activities, as these activities likely are more common than new construction.

Threat Level-Based Protocols

Feature 10—Water and wastewater utilities should monitor available threat-level information and escalate security procedures in response to relevant threats.

DHS regularly updates the national threat level in response to information about potential attacks. More specific information is also made available to utilities through secure information channels, such as the WaterISAC. Utilities should monitor this information so that they are aware of threats and can adjust security operations as needed. By providing for escalation of security operations in response to industry-specific threats and focusing security operations in response to specific threat information, utilities are better prepared to identify and potentially counter site-specific threats, and reinforce the expectation that security is a regular part of day-to-day operations.

The WSWG notes that there was a range of views in the Group about the relative utility of the national threat levels published by DHS—some members view these national threat levels as having very little relevance to utility operations; other members were less critical of the national threat levels. Despite this range of views on the national threat level system, the Group agreed that more specific information on utility-, facility- or region-specific threats or concerns is more useful and more important to monitor and that EPA and DHS should improve their efforts to provide updated, timely, actionable threat information to the water sector.

Secure alerts on threats and potential threats to water and wastewater utilities and other critical infrastructure are available to utilities through a number of national networks, including WaterISAC, the Water Security Channel, Infraguard, and through local networks, such as the Northwest Warning, Alert & Response Network (NW WARN). Other networks are being developed, including the SouthEast Emergency Response Network and the DHS Homeland Security Information Network (HSIN). Utilities should investigate what networks and information sources might be available to them locally, and at the state or regional level. The WSWG notes that, in some cases, it may be difficult for utilities to gain access to some information networks; where barriers exist, attempts should be made to align with those who can and will provide effective information to the utility.

Monitoring threat information should be a regular part of the security-program manager's job, and utility-, facility- and region-specific threat levels and information should be shared with those responsible for security and other key security staff. As part of security planning, utilities should develop systems to access threat information, procedures that will be followed in the event of increased industry or facility threat levels, and should be prepared to put these procedures in place immediately, so that adjustments are seamless. Enhanced security procedures might include, for example: notification to first responders that threat levels have increased; posting signs or otherwise notifying line staff and managers; and/or further reducing/controlling access to the utility or increasing contaminant monitoring.

Measure 10—Is there a protocol/procedure for responses to threat level changes?

By altering security practices in response to specific threats, utilities are better prepared to respond to events and reinforce security as a regular part of day-to-day utility operations. Feature 10 calls on utilities to monitor threat-level information, with an emphasis on information related to the utility and water sectors, and to escalate security procedures in response to increased threats as part of an active and effective security program. Measure 10 emphasizes the importance of the planning element associated with feature 10, by suggesting that utilities evaluate whether they are prepared to take appropriate action in response to changing threat information. The WSWG is not suggesting a specific threat threshold for action or specific actions to take. Utilities should identify the types of threat levels and information they will respond to, and the specific responses they will take, based on their specific circumstances and operating conditions.

Note that there was a range of views among WSWG members about the relative utility of the national threat levels published by the DHS. The Group does not assume utilities need to implement special security procedures in response to changes in the national threat level. The Group is more concerned about attentiveness to threats that are specific to a region, utility, or the water sector more generally. The WSWG also notes that threats need not be of a terrorist nature to prompt utilities to implement special security or other procedures. Many utilities have already developed special operational procedures that can be put in place in response to storms or other natural disaster threats. These procedures might be used as the basis for special security procedures.

Emergency Response and Recovery Plans

Feature 11—Emergency response and recovery plans should incorporate security considerations, be tested and reviewed regularly, and updated as necessary to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.

Emergency response and recovery plans describe who will do what in the event of an emergency. They are the critical document for establishing emergency response and recovery roles and priorities, and for assuring the continued safety of utility operations during and immediately after an emergency response. Over time, the conditions that defined utilities' initial emergency response and recovery plans will change; their plans and priorities should be changed and updated accordingly.

This feature establishes the expectation that utilities should incorporate security considerations into their emergency response and recovery plans, and should maintain these plans as "living documents." In incorporating security considerations into their emergency response and recovery plans, utilities also should be aware of the National Incident Management System (NIMS) guidelines, established by DHS, and of regional and local incident management commands and systems, which tend to flow from the national guidelines. Adoption of NIMS is required to qualify for funds dispersed through the DHS Office of State and Local Government Preparedness and Coordination. As of the writing of this document, more information on NIMS is available at http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf.

The timing for review and updating of emergency response and recovery plans will vary across utilities, depending on the degree to which security-related conditions are changing and any applicable state-level planning requirements. Utilities should consider their individual circumstances and establish, develop, and implement a schedule for review and update of emergency response and recovery plans that are appropriate to their circumstances. At a minimum, the WSWG believes that all utilities should review and (as needed) update their emergency response and recovery plan at least once every year. Conditions that might prompt more frequent review of emergency response and recovery plans include major facility construction projects, adding new facility infrastructure (by construction or acquisition), new response protocols in related critical infrastructure (such as the electric power sector), changes in response protocols or capabilities of emergency response organizations, and new information about specific threats.

Utilities also might find it useful to review emergency response and recovery plans after any event that causes the plan to be implemented—so that lessons learned from the event response can be incorporated into the plan and used in the future. Many utilities have found it useful to update their emergency response and recovery plans on a "page basis" to ensure strict tracking of versions and to ensure that all responders have up-to-date information. Using this approach, replacement plan pages would be sent to all responders at least once per year when plans are reviewed and updated.

The WSWG emphasizes that emergency response and recovery plans and planning should include not just the details of response activities, but also a discussion of the circumstances that would prompt implementation of the plan and who will make decisions about plan implementation. Utility plans should be thoroughly coordinated with emergency response and recovery planning in the larger community. Coordination is important, not just with response organizations, but also with other critical infrastructure sectors, such as electric power and public health providers. Coordination and education related to emergency response and recovery planning are also important for utility customers. Some utilities have found it helpful for customers to be aware that their utility has an emergency response and recovery plan in place and to have information on what, if

anything, the plan might call for them to do. For example, if plans call for customers to be asked to boil water under certain circumstances, they will be more likely to correctly carry out this precaution if they have advance information preparing them for the possibility. Some utilities have formed relationships with local public health providers and the Red Cross to prepare public service announcements and other education information about response to utility emergencies.

This feature also establishes the expectation that utilities should test or exercise their emergency response and recovery plans regularly. Plans might be tested through training and tabletop drills and exercises, or through real-time simulated responses. The WSWG believes it is particularly helpful to carry out these tests in concert with representatives of critical interdependent infrastructure sectors and with first responders. Some utilities have found it useful to participate in routine meetings of individuals with security, response, or law enforcement responsibilities. Establishing these collaborative partnerships helps in developing and facilitating implementation of emergency response and recovery plans. It also provides a routine, relatively informal mechanism to trade up-to-date information on threats and potential threats, security approaches, and response plans and capabilities. Utilities may wish to refer to the EPA *Tabletop Exercise Planning Guide for Public Drinking Water Systems* (January 2005) for additional information on planning and implementing tabletop exercises.

Measure 11—Are exercises regularly conducted that address the full range of threats—physical, cyber, and contamination—and is there a protocol/procedure to incorporate lessons learned from exercises and actual responses into updates to emergency response and recovery plans?

Feature 11 establishes the expectation that utilities will incorporate security considerations into their emergency response and recovery plans, that plans will be tested and reviewed regularly, and that plans will be updated as needed to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations. This measure emphasizes the importance of testing and exercising emergency response plans by suggesting that utilities evaluate whether exercises address the full range of physical, cyber, and contamination threats. It also reinforces the need for emergency response and recovery plans to be maintained as "living documents," by suggesting that utilities evaluate whether they are prepared to incorporate lessons learned from exercises and response into plan updates. Consistent with its focus on ongoing improvement in security programs (see Finding 6), the WSWG believes strongly in the importance of ongoing, thoughtful reassessment as a way to keep security programs "fresh" and effective, take advantage of emerging approaches and new technologies, and perpetuate a security culture throughout an organization.

Internal and External Communications

Feature 12—Water and wastewater utilities should develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, and customers.

This finding establishes the expectation that utilities should develop and implement communication strategies with key partners to increase security and be better prepared to respond to an emergency, whether caused by an accident, natural disaster, vandalism, or terrorist attack. Training utility workers and inviting community members to recognize and report unusual or suspicious events or activities is one of the best ways that utilities can improve their security posture. During an emergency, rapid, confident response may be critical to safeguarding public and environmental health. One of the keys to both these outcomes is communication.

The WSWG believes that effective communication strategies consider key messages; who is best equipped/trusted to deliver the key messages; the need for message consistency, particularly during an emergency; and the best mechanisms for delivering messages and for receiving information and feedback from key partners. These elements likely will vary depending on the audience with whom a utility is trying to communicate. The WSWG highlights three key audiences for communication strategies: utility employees, response organizations, and customers.

With respect to utility employees, reliable, ongoing communication strategies are a key part of creating an active and effective security culture. Communications strategies should maintain employee security awareness, motivate staff to take security seriously, provide ways for staff to notify appropriate security or other personnel about unusual or suspicious events or activities, ensure employee safety during an event, and enable effective employee participation during event response. This might be accomplished through regular security awareness briefings and the incorporation of security considerations into regular training activities. Efforts need to ensure that staff can distinguish between normal and unusual activity (both on and off site and in their professional and personal lives), understand how to notify management of suspicious activity, understand the nature of and restrictions on access to sensitive information and facilities, understand event-related safety procedures, and participate effectively in event response activities.

With respect to response organizations, communication strategies should focus on ensuring clarity and reliability in the event of an emergency. As discussed under feature 8, in the event of an emergency, conventional telecommunications networks will come under severe pressure and may fail. In this context, utilities should evaluate the need and means for providing back up systems that will enable maintaining contact with police, fire, and other first response organizations, as well as maintaining internal communication with employees to ensure safety and to coordinate response activities.

With respect to customers, communication strategies should especially consider the most effective ways to reach consumers with information, both in terms of delivery mechanism and source, and of providing a mechanism for customers to communicate with appropriate security or other personnel about unusual or suspicious events or activities. For example, some customers may be more inclined to pay attention to information that comes from the public health community than information that comes from a utility. Some delivery mechanisms might work well for customers who are at home during the day, but other mechanisms might be needed for customers who work during the day, or travel frequently. In the event of an emergency, plans should be in place to reliably disseminate information to people who need it, even if normal communication mechanisms are compromised. Some utilities have found it useful to invest in ongoing outreach and communication with customers to build trust, partnership, and open lines of communication well in advance of any service-related problem or security emergency.

Communication strategies also should address who is authorized to speak for a utility in the event of an emergency and ensure that person has pre-prepared communication materials and messages that can be tailored to the specifics of an event. It may be helpful to practice communication strategies and messages with local political leaders who will have a role in public communication during an actual public health emergency, before an emergency occurs. This will ensure that local political leaders have accurate expectations about how an actual public health emergency will be handled, and will reduce the likelihood that the public could receive mixed or conflicting messages.

Measure 12—Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns, and is there an up-to-date list and protocol for contacting emergency response partners?

The WSWG strongly believes that effective two-way communication within utilities and between utilities and their partners and customers in surrounding communities is one of the most important assets of an active and effective security program. Feature 12 describes in detail the WSWG's thoughts on the importance of internal and external communication, and expectations for communication efforts in active and effective security programs. Measure 12 highlights one of the main reasons the WSWG believes communication is important: effective communication strategies can dramatically increase a utility's ability to identify utility-specific security threats. Training utility workers and inviting community members to recognize and report unusual or suspicious events and other security concerns is one of the best ways utilities can improve their security posture. Residents who live near utility infrastructure and observe comings and goings on a daily basis are often best able to notice changes that may signal an increasing threat.

The WSWG is not prescribing a specific method utilities should use to provide for notification; utilities should develop notification strategies best suiting their particular circumstances, communities, and operating conditions. Over time, it also will be important for utilities to evaluate the effectiveness of communication mechanisms to ensure that mechanisms are working—this could be done by surveying or testing of communication mechanisms in tabletop or field exercises, or by evaluating whether a utility is acting on communication received through the communication mechanisms it has in place. For example, if a website is the communication mechanism for submitting concerns, it is an effective mechanism only if someone actually monitors, evaluates, and acts upon the submissions.

Note that by highlighting this element of internal and external communications, the WSWG is not intending to minimize other elements of this feature described earlier. In particular, the Group expects that as part of developing active and effective security programs, utilities will also develop and implement strategies to ensure reliable and clear communication during emergencies.

Partnerships

Feature 13—Water and wastewater utilities should forge reliable and collaborative partnerships with the communities they serve, managers of critical interdependent infrastructure, and response organizations.

During an actual response is not the opportune time to begin to develop good working relationships with managers of interdependent infrastructure, such as power supply or first responders. Utilities should identify and reach out to key partners—including communities, managers of interdependent infrastructure, public health officials and providers, and first responders—in advance of an emergency, so they are better prepared to work together if an emergency should occur. The objective of developing reliable, collaborative partnerships with these key partners is to improve security across interdependent infrastructures, improve vigilance toward security concerns, and improve responsiveness in the event of an attack.

Effective partnerships not only build collaborative working relationships, they also clearly define roles and responsibilities, so that people can work together seamlessly if an emergency should occur. These partnerships are essential to a utility's ability to enhance security and to respond effectively to emergencies. Developing reliable and collaborative partnerships involves reaching out to managers and key staff in other organizations to build understanding of their security concerns and planning, and to share information about the utility's security

concerns and planning. It is important to emphasize the need for reciprocity in these relationships—it is just as important for the utility to understand and be able to work with the power sector as it is for the power sector to understand and be able to work with the utility.

In many cases, reaching out to interdependent infrastructure and response organizations may have unforeseen benefits to daily operations. For example, one utility has worked with the local police and fire departments to enter information on its critical infrastructure into the police and fire secure global positioning system, so that police and fire responders are automatically notified of the presence of water utility infrastructure within 1000 yards of a response call. This day-to-day interaction has increased awareness of, and attentiveness to, water infrastructure in a way that will automatically increase security. In another case, arrangements were made for a 24-hour on-call utility worker to stay at a local firehouse with the 24-hour on-call fire personnel. This enabled the city to dispatch the utility worker for hydrant vandalism, rather than sending a fire truck, which saved the fire department time and money. The utility benefited from better accommodations for their worker and a closer, more collaborative relationship with the fire department.

It is also important for utilities to develop partnerships with the communities and customers they serve. Partnerships help to build credibility within communities and establish public confidence in utility operations. In the event of an emergency, these relationships likely will provide a foundation of common understanding and trust upon which confidence can be restored. Partnerships with communities also can provide real-time security enhancements, particularly for rural and ex-urban utilities. People who live near utility infrastructure can be the eyes and ears of the utility, and can be encouraged to notice and report changes in operating procedures or other suspicious behaviors. Neighborhood watches and other programs can help customers feel connected to the utility, make them aware of security considerations, and enhance both community partnership and security, at little cost. Effective community partnerships can have the important collateral benefit of increasing public support for security improvements and security-related spending, and any associated inconveniences (such as construction sites) or rate increases.

Measure 13—Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, and response organizations been established?

Partnerships are a natural outgrowth of effective communications; effective partnerships will improve security across interdependent infrastructure, improve vigilance towards security concerns, and improve the speed and quality of emergency response. Feature 13 establishes the expectation that utilities will forge reliable and collaborative partnerships with the communities and customers they serve, managers of critical interdependent infrastructure, and response organizations, as part of establishing active and effective security programs. This measure suggests utilities evaluate the quality of these partnerships.

The WSWG emphasizes the importance of utilities undertaking a critical and thoughtful evaluation of partnerships as part of this measure. The Group is not suggesting a specific method to evaluate partnerships; however, it strongly encourages utilities to engage partners in a dialogue as part of evaluation and to provide a forum in which partners can offer informed and candid observations and suggestions for improvement. As discussed earlier in this document, the WSWG is suggesting these measures as part of utility-specific self-assessment programs. Utilities should use the opportunity that self assessment provides to be realistic and thoughtful about their performance and opportunities to further improve their security posture.

Measures and Self Assessment

Feature 14—Water and wastewater utilities should develop utility-specific measures of security activities and achievements, and should self assess against these measures to understand and document program progress.

It is an axiom of modern organizations that what gets measured gets done. As part of an active and effective security program, water and wastewater utilities should develop utility-specific measures that can be used to understand and track progress, activities, and achievement. Measures should be appropriate to utility-specific circumstances and operating conditions, and should reflect the specific security approaches and tactics a utility has chosen. Measures help a utility verify that an active and effective security program is in place and help to document program outcomes. Although each utility's measures will be different, just as each utility's specific security approaches and tactics will be different, the WSWG suggests that utilities consider measures of a number of common types of activities and achievements, including the following.

- *Existence of program policies and procedures*. The WSWG anticipates that, as part of their specific security approaches and tactics, most, if not all, utilities will choose to develop some policies and procedures related to security. For example, as part of developing an explicit, visible commitment to security (feature 1), many utilities may choose to develop an overarching security policy. As part of intrusion detection and access controls (feature 6), many utilities may choose to develop employee and visitor identification procedures and access limitations. Where utilities have chosen to develop policies and procedures as part of their specific security program approaches or tactics, the existence of these policies and procedures should be documented as part of implementing an active and effective security program.
- *Training*. The WSWG anticipates training on security approaches and tactics will be part of most, if not all, utility security programs. Where security-related training is planned, utilities should measure whether the training has been carried out as planned and the effectiveness of training as part of implementing an active and effective security program.
- *Testing*. As a complement to documenting where security-related policies and procedures are in place, utilities should test and measure whether staff (including contractors) are operating consistently with established security-related policies and procedures, and whether the policies and procedures result in effective operations, response, and communication. These tests can take a variety of forms, including observing staff activity, retroactive review of security related activities, tabletop and field exercises, and review of lessons learned from security activities and emergency responses.
- *Implementing schedules and plans*. As part of developing an active and effective security program, individual utilities will develop utility-specific schedules and plans. For example, utilities will develop schedules and plans for carrying out regular updates to assessments of vulnerabilities (feature 3) and emergency response plans (feature 11). Where these schedules and plans are in place, utilities should measure whether they carry out updates in accordance with schedules and plans.

In addition to suggesting that utilities establish utility-specific measurement and self-assessment programs, the WSWG suggests a number of specific security measures that apply across the full range of utility circumstances and operating conditions (see Finding 16). The Group emphasizes that these measures are intended to form the basis of a utility-specific measurement program, not replace utility-specific measures.

Once security measures are in place, utilities should regularly conduct self assessments of their security programs and track progress against their measures. At a minimum, the WSWG believes self assessments should be done annually, as part of an annual security program review. The WSWG reiterates that self assessment should be based on consideration of the specific measures a utility has put in place. The Group

does not assume that self assessment will include annual conduct of a full assessment of vulnerabilities, although some utilities may choose to update their assessments of vulnerabilities annually. The WSWG also suggests establishing a voluntary, utility security peer technical assistance and review process to complement, as individual utilities deem desirable, utility self assessments (see Finding 11).

APPENDIX B: CHART SHOWING FEATURES OF AN ACTIVE AND EFFECTIVE SECURITY PROGRAM AND CORRESPONDING MEASURES THAT UTILITIES SHOULD USE

#	Feature	Measure
1.	Water and wastewater utilities should make an explicit and visible commitment to security.	Does a written, enterprise-wide security policy exist, and is the policy reviewed regularly and updated as needed?
2.	Water and wastewater utilities should promote security awareness throughout their organizations.	Are incidents reported in a timely way, and are lessons learned from incident responses reviewed and, as appropriate, incorporated into future utility security efforts?
3.	Water and wastewater utilities should assess vulnerabilities and periodically review and update vulnerability assessments to reflect changes in potential threats and vulnerabilities.	Are reassessments of vulnerabilities made after incidents, and are lessons learned and other relevant information incorporated into security practices?
4.	Water and wastewater utilities should identify security priorities and, on an annual basis, identify the resources dedicated to security programs and planned security improvements, if any.	Are security priorities clearly identified, and to what extent do security priorities have resources assigned to them?
5.	Water and wastewater utilities should identify managers and employees who are responsible for security and establish security expectations for all staff.	Are managers and employees who are responsible for security identified?
6.	Water and wastewater utilities should establish physical and procedural controls to restrict access to utility infrastructure to only those conducting authorized, official business and to detect unauthorized physical intrusions.	To what extent are methods to control access to sensitive assets in place?
7.	Water and wastewater utilities should employ protocols for detection of contamination consistent with the recognized limitations in current contaminant detection, monitoring, and surveillance technology.	Is there a protocol/procedure in place to identify and respond to suspected contamination events?
8.	Water and wastewater utilities should define security-sensitive information, establish physical and procedural controls to restrict access to security-sensitive information as appropriate, detect unauthorized access, and ensure information and communications systems will function during emergency response and recovery.	Is there a procedure to identify and control security-sensitive information, is information correctly categorized, and how do control measures perform under testing?
9.	Water and wastewater utilities should incorporate security considerations into decisions about acquisition, repair, major maintenance, and replacement of physical infrastructure; this should include consideration of opportunities to reduce risk through physical hardening and the adoption of inherently lower risk design and technology options.	Are security considerations incorporated into internal utility design and construction standards for new facilities/infrastructure and major maintenance projects?
10.	Water and wastewater utilities should monitor available threat-level information and escalate security procedures in response to relevant threats.	Is there a protocol/procedure of responses that will be made if threat levels change?

#	Feature	Measure
11.	Emergency response and recovery plans should incorporate security considerations, be tested and reviewed regularly, and updated as necessary to reflect changes in potential threats, physical infrastructure, utility operations, critical interdependencies, and response protocols in partner organizations.	Do exercises address the full range of threats—physical, cyber, and contamination—and is there a protocol/procedure to incorporate lessons learned from exercises and actual responses into updates to emergency response and recovery plans?
12.	Water and wastewater utilities should develop and implement strategies for regular, ongoing security-related communications with employees, response organizations, and customers.	Is there a mechanism for utility employees, partners, and the community to notify the utility of suspicious occurrences and other security concerns?
13.	Water and wastewater utilities should forge reliable and collaborative partnerships with the communities they serve, managers of critical interdependent infrastructure, and response organizations.	Have reliable and collaborative partnerships with customers, managers of independent interrelated infrastructure, and response organizations been established?
14.	Water and wastewater utilities should develop utility-specific measures of security activities and achievements and should self assess against these measure to understand and document program progress.	Not applicable.

APPENDIX C: ADDITIONAL MEASURES UTILITIES SHOULD CONSIDER

During their deliberations to identify measure that all utilities should use, the WSWG identified numerous other potential measures of active and effective security programs. The measures suggested above for all utilities to use are the minimum necessary to create a foundation for a successful utility security self-assessment and measurement program. Utilities should supplement the measures suggested above with additional measures that reflect the specific security approaches and tactics they have chosen and that are appropriate to their specific circumstances and operating conditions.

This appendix lists measures that the WSWG considered during its deliberations and that it suggests utilities should consider when developing a utility-specific self-assessment and measurement program. While not all the measures listed here will be applicable to every utility, they cover many of the elements of a successful measurement program that the WSWG suggested earlier (existence of program policies and procedures, training, testing/exercising, and implementing schedules and plans; see feature 14) and represent the WSWG's best thinking on what would constitute sound measures.

Feature 1—Explicit Commitment to Security

- Are written security policies and procedures established? (y/n)
- Are procedures/protocols updated routinely? (y/n)
- Is there a public education program for customers and public officials? (y/n)
- Are agreements with emergency response partners in place? (y/n)
- Is there an explicit commitment to security? (y/n)
- Does the commitment to security address the full scope of the security program? (y/n)

Feature 2—Security Culture

- Are all management and staff security trained? (y/n)
- Is there documentation of incidents and associated responses? (y/n)
- How many incidents/suspicious incidents are reported? (Measure raw number of incidents and changes in the number of incidents over time.)
- Are incidents and responses reviewed with staff? (y/n)
- Are lessons learned from incidents and incident response incorporated into future planning? (y/n)
- Are there incidents that were not reported or not reported in a timely way and, if so, how many? (y/n and number)
- Were responses to incidents consistent with established policies and procedures? (y/n)
- Are there efforts to promote security awareness throughout the utility? (y/n)
- Are security policies and procedures followed? (y/n)
- Is there a process/protocol by which suggestions for security improvements can be made by employees and the public? (y/n) How many suggestions are made? Are suggestions followed up on in a timely way? (y/n)
- Is there a way to keep up to date on security improvements and good security practices/models from other utilities? (y/n)

Feature 3—Up-to-Date Assessment of Vulnerability

- Is there a procedure or protocol that establishes an internal periodic reassessment of vulnerability (including design basis threat) and a schedule for this reassessment? (y/n)
- Is the periodic reassessment done? (y/n)
- Is it done on schedule? (y/n)
- Is a reassessment of vulnerabilities conducted after incidents? (y/n)
- Is follow-up conducted after each reassessment to incorporate changes, lessons learned, and security improvements into security practices? (y/n)
- Are conditions that drive changes in vulnerability identified and tracked? (y/n)
- Are reviews of vulnerability carried out by a team of employees from both security and operations? (y/n)

Feature 4—Dedicated Security Resources and Security Implementation Priorities

- Are solutions to vulnerabilities (steps to take to reduce vulnerabilities or reduce potential consequences) identified and built into the security plan (y/n), prioritized (y/n), and given a time frame to complete (y/n)?
- Have solutions to vulnerabilities and measures to mitigate potential consequences been considered and evaluated for importance and ability to fund, and funding decisions been made? (y/n)
- Do solutions to vulnerabilities and measures to mitigate potential consequences have resources assigned to them? (Measure number and type with assigned resources and total percentage with resources assigned.)
- What number of high-priority security improvements (solutions to vulnerabilities) have been addressed? (Measure raw number of vulnerabilities addressed.)
- How many milestones have been accomplished from the security plan? (Measure raw number of accomplishments.)
- How many capital improvement dollars have been spent on security? (Measure raw dollar amount.)
- How many operational improvements have been made? (Measure raw number of improvements.)
- How many changes have been made in maintenance activities? (Measure raw number of activities.)
- Are the skills needed to implement security improvements identified and available? (y/n)
- Are resources dedicated to security identified on an annual basis? (y/n)
- Are planned security improvements, if any, identified? (y/n)

Feature 5—Defined Security Roles and Employee Expectations

- Does management/utility board support adoption of security policies? (y/n)
- Are security roles/responsibilities included in job descriptions, employee evaluations, or other documentation of responsibilities? (y/n)
- Does staff receive training relative to their security roles/responsibilities (y/n) and is the training ongoing (y/n)?
- Is performance of security roles/responsibilities part of performance evaluations? (y/n)
- Have managers and employees who are responsible for security been identified? (y/n)
- Are background checks performed for current and new employees, including contractors? (y/n)
- Are there means to readily identify all employees, contractors, and visitors? (y/n)

Feature 6—Intrusion Detection and Access Control for the Physical Plant

- Is there a procedure/protocol on intrusion detection and access control? (y/n)
- Are the procedures/protocols tested regularly? (y/n)
- Are non-public spaces protected from casual trespass? (y/n)

- Is there a way to control access to sensitive assets? (y/n)
- Is a security perimeter established (y/n) and is there technology to monitor the established security perimeter (y/n)?
- Are all utility employees and contractors identified? (y/n)
- Are visitors to the utility checked in and escorted? (y/n)
- Is access denied to persons who no longer qualify for access? (y/n)
- Can individuals who are not eligible for access talk their way in to restricted areas? (y/n)
- Is there a means to control vehicular access? (y/n)
- Are intrusions detected and responded to in a timely way? (y/n)
- Are there policies and/or procedures for monitoring chemical delivery schedules and safeguarding chemical deliveries? (y/n)
- Are the chemical delivery policies/procedures tested regularly? (y/n)

Feature 7—Contamination Detection

- Is there a system of monitoring for contaminant detection? (y/n)
- What type of monitoring is being used? (describe)
- Is there a system to keep up-to-date on emerging technologies for contamination detection and monitoring? (y/n)
- Have connections been established with public health networks to detect, interpret, and act upon public health anomalies? (y/n)
- Are customer complaints monitored and evaluated for possible indications of contamination events? (y/n)
- Have protocols been established for interpreting and responding to indications of public health anomalies? (y/n)

Feature 8—Information Protection and Continuity

- Are there policies and procedures in place that categorize and control security information? (y/n)
- Are these policies used/followed? (y/n)
- Is there a training program for information security policies/procedures? (y/n)
- Is there regular testing of information security policies/procedures? (y/n)
- How does implementation of the policies and procedures perform under testing—is information secure? (Measure performance against testing benchmarks.)
- Are documents correctly categorized relative to security content? (y/n and measure number and percentage correctly categorized.)
- Is there a dedicated lead information officer for both paper and electronic information? (y/n)
- Is there an employee training program for information security and, if so, how many employees have been trained? (y/n and number)
- Is security incorporated into design standards for new information systems? (y/n)
- Can the IT firewall be breached? (Measure number of total attempts and number and percentage of attempts that are wholly or partially successful.)
- Are information security considerations incorporated into decisions about design and acquisition of new systems or updates to current systems? (y/n)

Feature 9—Design and Construction

- Is there a protocol in place for examining the potential multiple benefits of design choices, with an emphasis on designs that more fully address security? (y/n)
- Have security considerations been incorporated into internal utility design and construction standards? (y/n)
- Do these standards include consideration of opportunities to reduce both security and safety risk through the adoption of inherently lower-risk design and technology options? (y/n)
- Are there policies/procedures in place to ensure that facilities remain secure during construction? (y/n)
- Is there a training program on these policies/procedures and, if so, how many employees have been trained? (y/n and number)
- Are these policies/procedures tested regularly? (y/n)
- Is security considered in both design of new facilities/infrastructure and in major maintenance projects? (y/n)

Feature 10—Threat-Level Based Protocols

- Is an active system in place to identify and assess threat level changes, with an emphasis on geographic- and industry-specific threats? (y/n)
- Is a list of sources of threat level information created/updated? (y/n)
- Has the utility developed procedure/protocol of responses that will be made if threat levels change? (y/n)
- Are responses undertaken when needed? (y/n and measure the percent of times correct response undertaken.)
- How much time does it take to make change in protocol relative to established objective? (Measure time and change in time over time.)

Feature 11—Emergency Response and Recovery Plans Tested and Up-to-Date

- Does the emergency response and recovery plan incorporate security-related threats and responses consistent with the assessment of vulnerabilities? (y/n)
- Is response staff identified and trained? (y/n)
- What were the results of planned and unplanned drills/exercises? (Measure quality of response.)
- Do exercises set specific objectives and test them? (y/n)
- How long does it take for full organization to fully mobilize relative to established objective? (Measure time and change in time over time.)
- How long does it take for individuals to mobilize relative to established objective? (Measure time and change in time over time.)
- Is there a high, medium, or low rating of coordination with other responders during an exercise? (Measure with survey results.)
- How well do exercises test performance?
- Are there protocols/procedures to incorporate lessons learned from exercises and actual responses into updates to the emergency response and recovery plan? (y/n)
- Do exercises address the full range of threats—physical, cyber, and/or contamination? (y/n)
- Are security considerations incorporated into emergency response plans? (y/n)
- Are emergency response and recovery plans updated in response to changes in security considerations? (y/n)
- Do emergency response and recovery plans reflect an awareness of the National Incident Management System Guidelines? (y/n)
- Has a schedule for review, reflective of individual utility security-related conditions, been established? (y/n)
- Has the emergency response and recovery plan been reviewed at least once per year? (y/n)

- Were emergency response and recovery plans reviewed and updated as needed in response to such changes as major facility construction projects, new facility infrastructure, and/or new information regarding threats? (y/n)
- Is the emergency response and recovery plan thoroughly coordinated with emergency response planning in the larger community? (y/n)
- Has the emergency response and recovery plan been tested regularly and, if so, when was the last test? (y/n and date)
- Are there contingency plans in place in case of failure of primary response systems or partnerships? (y/n)

Feature 12—Internal and External Communication

- Has a list of organizations/individuals to communicate with established? (y/n)
- Has a schedule/cycle of contact established? (y/n)
- Has that schedule of contacts been met or exceeded? (y/n and measure percent of contacts met or exceeded on schedule)
- Do partner organizations know what the utility thinks they should know? (Measure with survey data.)
- Is the community aware of its role in improving security and what to watch for? (y/n)
- Is there a mechanism for employees to make suggestions for security improvements? (y/n)
- Is there a mechanism for employees to get information about security practices? (y/n)
- Are security issues included as part of routine employee briefings and staff meetings? (y/n)
- Is information disseminated to employees, as appropriate, when security practices change? (y/n)
- Is information disseminated to employees, as appropriate, when threat levels change? (y/n)
- Is there redundancy in communication technologies? (y/n)
- Is there a way for partners and the community to make suggestions for security improvements? (y/n)
- Is there a way for partners and the community to notify the utilities of suspicious occurrences or other security concerns? (y/n)

Feature 13—Partnerships

- Are key partners identified? (y/n)
- Has a joint communications plan been established? (y/n)
- Have communications been undertaken consistent with the plan? (y/n)
- How many meetings with responders have taken place per year? (Measure raw number.)
- Have the needs of partners been met in joint exercises? (Measure with survey data.)
- Have reliable and collaborative partnerships with served communities, managers of interdependent infrastructure, and response organizations been established? (y/n)

APPENDIX D: INDIVIDUAL COMMENTS OF WSWG MEMBERS

Comments of Nick Catrantzos

Security for Water: A Personal Distillation

By
Nick Catrantzos, CPP

Security matters. Even the simplest efforts can make a difference. Yet unfunded mandates can dissuade the very action they are intended to encourage. Ideas like these supplied context and debating points in a year of Water Security Working Group deliberations. By the end of the year, good ideas and common ground emerged. Here are the personal lessons I distilled along the way.

Know Your World

Before we can speak intelligently about protecting critical infrastructure, we must know what we want to protect. At the strategic level, we must identify and prioritize our critical assets. Yet we must also evaluate options for protecting them, on the one hand, and for reducing the impact of their loss, on the other hand. A risk or vulnerability assessment is a handy tool for making us think these things through. This process is valuable, no matter the methodology used. We also need to refresh this process and our conclusions from time to time. Why? Threats change. Today's critical asset becomes tomorrow's back-up system or museum relic. Security options improve, too. Finally, at the day-to-day, micro level, we must all be alert to our surroundings. Only the people who work daily at a given site or in a given operation can recognize what does not belong there. To recognize what is suspicious or out of place, we must remain aware. We must know our world.

Start Somewhere

It is very easy to spend more time complaining about some aspect of security than to actually take a first step in protecting assets. Avoid assuming that every imperfection represents a fatal flaw. Perfect security is an illusion. Perfect security would require bringing all operations to a halt in order to safeguard them. It would mean going out of business to protect the business. Because security can be interpreted so broadly as to affect everything, it is easy to consider it daunting. It may also be tempting to refuse to do anything without an extra funding source. This approach is a recipe for inaction.

Security is never convenient. But it need not break the bank. Just as most people think nothing of carrying keys and locking their homes, security works best and is easiest to take when integral to our daily lives. It only becomes oppressive if treated as an appliqué or transformed into an impossible dream.

There are no easy answers. Yet improvement is always possible, even with limited budgets. It is important to start somewhere. Controlling access to critical facilities, for example, is always possible on some level. This, plus a security awareness message to employees to watch for and report intruders, plus a good example by leaders following security rules turns into a basic security program. It is an example of adding value without waiting for outside influence. Many smaller utilities have already figured this out, outperforming larger entities.

At Least Ask

There is a management adage that says what gets inspected is what gets respected. Even if you cannot afford an extra dollar for security, you can still do better. How? Ask if your own procedures are really being followed. Often, exploited vulnerabilities are those others in the organization knew about. Maybe they did not tell anyone. Or maybe they did, but no one listened. Or maybe just too much time passed since someone cared enough to inquire. If you cannot do anything else, at least ask.

Closing Observations

This report is necessarily imperfect. Yet it is comprehensive, thanks to the exceptional work of the Ross and Associates facilitation team that toiled indefatigably to canvass all views of WSWG members, no matter how wide-ranging. Ross's Elizabeth McManus and Rob Greenwood, in particular, mastered a kind of magic that regularly translated argot into the vulgate and forced us to make sense when too much brainstorming left us awash in good ideas without the necessary bridge to practicality. It is also a tribute to the finesse of two bright and sophisticated co-chairs, Rebecca Head and Dave Binning, who routinely rescued us when mired in minutia.

One consistent value for the reader is that every suggestion or feature has been fire-tested in at least one crucible. Nothing is a cure-all. Nor is it intended to substitute for common sense and informed management. A utility could follow all the recommendations to the letter and, lacking true commitment, still fall short of protecting the critical infrastructure under its stewardship. Conversely, another utility could defend its infrastructure superbly, yet only pick and choose sparingly from the recommended menu we offer.

Nevertheless, addressing the features and suggestions in this report requires thinking about security at all levels of the organization. And this is where the greatest value comes. In our busy worlds, where security is still competing for attention, it is by no means the core business. This report succeeds when it generates serious thought and even debate about security, without doing so at the expense of core business. Periodically. Regularly. And, eventually, instinctively. At the end of the day, the message we deliver is that good security is good business.

Respectfully submitted,

Nick Catrantzos

Nick Catrantzos, Certified Protection Professional (CPP)
Security and Emergency Manager
Metropolitan Water District of Southern California

These comments reflect the opinion/perspective of the Department of Defense (DoD) Federal Partner (Major Timothy Mukoda, USAF) and do represent an official DoD position. These comments will not be recognized as an official DoD position until/unless they have been formally staffed and coordinated through all Services (US Air Force, US Army, US Navy, US Marine Corps).

Active and effective drinking water and wastewater security programs are directly related to overall National Security. Two of the primary motivating factors that should drive effective and efficient program implementation are:

1) The ethical responsibility for ensuring protection of public health and welfare;
2) Developing and maintaining customer/consumer confidence.

Regulation of a water security program has the potential to be counterproductive to effective program implementation. First, regulation at the Federal or state level may drive requirements that are not applicable at the local level. Second, current programs that are effective but do not meet strict compliance requirements may be forced to adjust in ways that contribute no overall value. Finally, mandatory compliance-related activity may result in unintended consequences regarding use of resources to meet compliance. This last point is critical to consider in a resource-constrained environment.

It is important that any guidance related to active and effective water security programs remain in the realm of "guidance". This provides a general roadmap for ultimate success, but does not dictate the exact route by which success may be achieved. Most, if not all, water utilities will have adequate incentive to lean forward and implement water security programs tailored to local need based on the factors listed previously.

ATTACHMENT 1: ROSTER OF WSWG MEMBERS, FEDERAL RESOURCE PERSONNEL, AND OUTSIDE EXPERTS

National Drinking Water Advisory Council
Water Security Working Group

Contact Information

Co-Chairs

Mr. David Binning
Director
Planning & Engineering
Fairfax Water
8560 Arlington Boulevard
Fairfax, Virginia 22031
Phone: (O) 703-289-6325
dbinning@fairfaxwater.org

Dr. Rebecca Head*
Health Officer/Director
Monroe County Health Department
2353 Custer Road
Monroe, MI 48161-9769
Phone: 734-240-7800
rebecca_head@monroemi.org

Members

Mr. Doug Anderton
General Manager
Dade County Water & Sewer Authority
P.O. Box 1047
250 Bond Street
Trenton, Georgia 30752
Phone: (O) 706-657-4341
Phone: (C) 423-991-0096
danderton5@aol.com or danderton@tvn.net

Mr. Paul Bennett
New York City Department of Environmental Protection, Director of Security Planning
465 Columbus Ave
Valhalla, NY 10595
Phone: (O) 914-773-4512
pbennett@dep.nyc.gov

Honorable John W. Betkoski, III*
Commissioner
Connecticut Department of Public Utility Control
10 Franklin Square
New Britain, Connecticut 06501
Phone: 860-827-2803
john.betkoski@po.state.ct.us or assistant melissa.lupacchino@po.state.ct.us

Mr. Nick Catrantzos
Security & Emergency Manager
Metropolitan Water District of Southern California
700 N. Alameda Street
Los Angeles, California 90012
Phone: (O) 213-217-7134
ncatrantzos@mwdh2o.com

Mr. Jeff Cooley
Alabama State Coordinator
Community Resource Group, Inc.
Rural Community Assistance Program
1110 Hillcrest Road #2D
Mobile, Alabama 36695
Phone: (O) 251-776-6635
Phone: (C) 251-454-2978
jcooley@crg.org or crg-al@msn.com

Mr. Michael Gritzuk
Formerly, Director
City of Phoenix Water Services Department
200 W. Washington Street, 9th Floor
Phoenix, Arizona 85003-1611
Phone: (O) 480-951-1580
michaelgritzuk@yahoo.com

Mr. Gregg Grunenfelder
Chief Administrator
Environmental Health Division
Washington State Department of Health
P.O. Box 47820
Olympia, Washington 98504-7820
Phone: (O) 360-236-3053
gregg.grunenfelder@doh.wa.gov

Mr. H. J. "Bud" Schardein
Executive Director
Louisville & Jefferson County Metropolitan Sewer District
700 West Liberty Street
Louisville, KY 40203
Phone: (O) 502-540-6346
Email: bennett@msdlouky.org or assistant schardei@msdlouky.org

Ms. Jennifer Nuzzo
Center for Biosecurity
University of Pittsburgh Medical Center
The Pier IV Building
621 E. Pratt Street, Suite 210
Baltimore, Maryland 21202
Phone: (O) 443-573-3315
jnuzzo@upmc-biosecurity.org

Mr. Paul Orum
Senior Advisor
Working Group on Community Right-to-Know
PO Box 15465
Washington, DC 20003
Phone: (O) 202-548-4020
orum@crtk.org
paul_orum@yahoo.com

Mr. Roger Selburg
Manager
Division of Public Water Supplies
Illinois Environmental Protection Agency
P.O. Box 19276
Springfield, Illinois 62794-9276
Phone: (O) 217-785-8653
roger.selburg@epa.state.il.us

Mr. David Siburg
General Manager
Kitsap Public Utility District
PUD #1 of Kitsap County
1431 Finn Hill Road
P.O. Box 1989
Poulsbo, Washington 98370-0933
Phone: (O) 360-779-9163, ext. 703
Phone: (C) 360-620-7680
dave@kpud.org

Ms. Diane VanDe Hei
Executive Director, Association of Metropolitan Water Agencies
1620 I Street, NW, Suite 500
Washington, DC 20006
Phone: (O) 202-331-2820
vandehei@amwa.net

Mr. John S. Young, Jr.*
Vice President
Operations and Investment Performance
American Water Works Service Co., Inc.
1025 Laurel Oak Road
Voorhees, New Jersey 08043
Phone: 856-346-8250
jyoung@amwater.com

Designated Federal Official

Mr. Marc Santora
Environmental Protection Agency
Office of Ground Water and Drinking Water
Water Security Division, Security Assistance Branch
1200 Pennsylvania Avenue, NW
Room 2368J / Mail Code (4608 M)
Washington, DC 20460
Phone: (O) 202-564-1597
Fax: 202-564-8513
santora.marc@epa.gov

US EPA Federal Partners

Ms. Janet Pawlukiewicz
Environmental Protection Agency
pawlukiewicz.janet@epa.gov
202-564-3779

Mr. David Travers
Environmental Protection Agency
travers.david@epa.gov
202-564-4638

Ms. Debbie Newberry
Environmental Protection Agency
newberry.debbie@epa.gov
202-564-1415

Other Federal Partners

Dr. Richard Gelting
Centers for Disease Control and Prevention
Environmental Engineer
Environmental Health Services Branch
National Center for Environmental Health
4770 Buford Highway, Mail Stop F28
Atlanta, GA 30341
Phone: (770) 488-7067
Fax: (770) 488-7310
richard.gelting@cdc.hhs.gov

Mr. Mark D. Miller, R.S., M.P.H.
Alternate for Mr. Richard Gelting
Commander, U.S. Public Health Service
Senior Environmental Health Officer
Center for Disease Control and Prevention
National Center for Environmental Health
Environmental Health Services Branch
4770 Buford Highway, NE (F28)
Atlanta, Ga 30341-3724
Phone: 770-488-7652
Fax: 770-488-7310
mdmiller@cdc.gov

Mr. John Laws
Coordinator-Water / Wastewater-Dams Sector specialist, U.S. Department of Homeland Security, Information Analysis & Infrastructure Protection (IAIP), Infrastructure Coordination Division (ICD), Infrastructure Coordination Analysis Office (ICAO)
703-235-5404 New Office
703-883-7651 Office
887-205-6674 pager
703-883-4589 fax
John.laws2@dhs.gov
jlaws@mitre.org

Ms. Nancy Wong
Department of Homeland Security
Infrastructure Coordination Division
c/o Department of Commerce
1401 Constitution Avenue, NW
Suite 6095
Washington, DC 20230
Phone: 202-482-9055
Fax: 202-482-7499
nancy.wong1@dhs.gov

Mr. Timothy J. Mukoda, Maj, USAF, BSC
Chief, Environmental Operations
AFMSA/SGPE
110 Luke Ave, Room 405
Bolling AFB, DC 20032
Phone: (202) 767-4327
Fax: (202) 767-5053 (fax)
timothy.mukoda@pentagon.af.mil

Mr. Jasper Welsch,
Mississippi Emergency Management Agency
P.O Box 4501
Jackson, MS 39296-4501
Phone: 601-360-0055
Fax: 601-352-8314
jwelsch@msema.org

Facilitation Support Team

Mr. Rob Greenwood
Ross & Associates Environmental Consulting, Ltd.
1218 Third Avenue, Suite 1207
Seattle, WA 98101
Phone: 206-447-1805
Fax: 206-447-0956
rob.greenwood@ross-assoc.com

Ms. Elizabeth McManus
Ross & Associates Environmental Consulting, Ltd.
1218 Third Avenue, Suite 1207
Seattle, WA 98101
Phone: 206-447-1805
Fax: 206-447-0956
elizabeth.mcmanus@ross-assoc.com

Mr. Elijah Levitt
Ross & Associates Environmental
Consulting, Ltd.
1218 Third Avenue, Suite 1207
Seattle, WA 98101
Phone: 206-447-1805
Fax: 206-447-0956
elijah.levitt@ross-assoc.com

Mr. Ryan Orth
Ross & Associates Environmental
Consulting, Ltd.
1218 Third Avenue, Suite 1207
Seattle, WA 98101
Phone: 206-447-1805
Fax: 206-447-0956
ryan.orth@ross-assoc.com

ATTACHMENT 2: WSWG OPERATING PROCEDURES

National Drinking Water Advisory Council
Water Security Working Group

Final Operating Procedures

Establishment and Mission

The Water Security Working Group (WSWG) is established and charged by the National Drinking Water Advisory Council (NDWAC). The Mission of the WSWG is to provide findings to the NDWAC that:

> (1) identify, compile, and characterize best security practices and policies for drinking water and wastewater utilities and provide an approach for considering and adopting these practices and policies at a utility level;
>
> (2) consider mechanisms to provide recognition and incentives that facilitate a broad and receptive response among the water sector to implement these best security practices and policies, and make findings as appropriate; and
>
> (3) consider mechanisms to measure the extent of implementation of these best security practices and policies, identify the impediments to their implementation, and make findings as appropriate.

The WSWG rejected use of the term "best" to describe their work on security practices; instead, the Group will identify and describe the components of "active and effective" security programs for water and wastewater utilities. In addition, the WSWG interprets the scope of its deliberations to include all water and wastewater operations, from source water to tap and from collection system to discharge.

WSWG findings will be presented to the NDWAC for the Council's consideration. The WSWG will not issue findings directly to EPA or any other agency or entity, although, of course, individual members are not restricted from discussing their views as they so choose. Upon receipt of the WSWG findings, the NDWAC will consider the findings and may pass them to EPA unchanged, or may amend them to reflect their own views, or may choose not to forward findings to EPA.

Participants and Participation

Working Group members were selected by EPA from among more than 80 nominated individuals. Selections were made considering the expertise and experience needed to provide advice to the NDWAC (and, through the NDWAC, to EPA) on best security practices, incentives, and measures, and were based on the need to provide balanced and complete representation across the water sector. To facilitate communication between the NDWAC and the WSWG, three members of the NDWAC are also members of the WSWG.

Direct participation of all WSWG members is essential to the success of the Working Group. For that reason members are asked to make every effort to attend Working Group meetings and participate in Working Group conference calls. Members who are not able to attend a particular meeting or conference call may send an alternate. The alternate must be a peer of the WSWG member. In an emergency situation, an association staff

member may serve as an alternative; however, in accordance with the ground rules for NDWAC working groups, this will be allowed only once in the duration of the WSWG. Alternates may be asked to contribute to WSWG deliberations by offering their opinion and expertise; however, they will not participate in WSWG decision making.

WSWG members are encouraged to frame observations in terms of needs and interests, not in terms of positions; opportunities for finding solutions increase dramatically when discussion focuses on needs and interests. Collaborative problem solving depends on mutual respect and careful listening among members. Meetings and conference calls will be structured to support a respectful atmosphere, encourage the development of trust and understanding, and provide for participation of all WSWG members. WSWG members agree to act in good faith in all aspects of their deliberations and consensus building. Members agree to refrain from characterizing the views of other parties in general, and particularly in any discussions that they may choose to have with the press.

WSWG members are welcome to be accompanied to the meetings by staff or other personnel, who may observe the WSWG meeting and offer comments or observations consistent with the operating procedures for public observation and comment.

It is the expectation that all WSWG members will participate through the entire process and that the Working Group's final document will reflect the consensus or the range of views that exist within the group relative to best security practices, incentives, and measures. However, any party may withdraw from the Working Group at any time without prejudice. In the event a member decides to withdraw from the process, he or she will be respectfully requested to communicate the reasons for the withdrawal, and may be replaced by another representative of similar expertise and interest.

Co-Chairs

The WSWG will be served by two co-chairs. One of the co-chairs will be a member of the WSWG who is also a member of NDWAC. This individual will be identified by EPA and the facilitation team in consultation with all three of the NDWAC members who serve on the WSWG. The second co-chair will be a member of the WSWG who is identified by the Group using a weight of preferences model.

The role of the WSWG co-chairs is to act as a sounding board for the facilitation team between WSWG meetings, open and close the WSWG meetings, assist the facilitation team in running the meetings, and approve WSWG meeting summaries after the facilitation team has addressed comments by WSWG members. The co-chairs also participate in deliberations and decision making as full members of the WSWG. The co-chairs do not determine the WSWG agenda or findings any more or less than any other WSWG member.

Reporting to the NDWAC

The WSWG will identify which members of the Working Group will report to the NDWAC on the Group's findings. It is not assumed that the co-chairs will be the members of the WSWG who report to the NDWAC. WSWG members who are also members of the NDWAC may, in the course of discussions with the NDWAC, provide informal updates on WSWG deliberations and progress based on the final meeting summaries, speaking for themselves as members of the WSWG not representing the full Group. For the winter 2004 NDWAC meeting, the WSWG agrees that the three WSWG members who also are NDWAC members will provide an update to the NDWAC on WSWG activities and progress.

Facilitation

The Working Group will be supported by a neutral, third-party facilitation team. The facilitation role includes: developing draft agendas, meeting summaries, report documents, and other materials; running the WSWG meetings; focusing and facilitating Working Group discussions to ensure that the perspectives of all WSWG

members come forward; working with Working Group members and EPA between meetings and conference calls to support understanding and consensus building; working with Working Group members and EPA to identify, organize, synthesize, and provide information and other material needed to support Working Group deliberations; and, in general, coordinating Working Group activities.

Federal Resource Personnel and Outside Experts

In addition to the facilitation team, the WSWG will be supported by a number of resource personnel from federal agencies with interest and expertise in water security. This will include representatives from the Environmental Protection Agency (EPA), Department of Homeland Security (DHS), Department of Defense (DoD), and the Centers for Disease Control and Prevention (CDC). As needed, and as resources allow, the Working Group also may choose to consult with, or the facilitation support team may identify, additional outside experts or individuals on specific subject matters. To date, one outside expert, an individual with technical expertise in emergency response, has been identified.

Federal resource personnel and outside experts may sit at the table during WSWG meetings so as to be easily accessible to Working Group members and may make presentations to the WSWG; however, their support of Working Group discussions is strictly to provide background, context, or other information or expert opinion, as called upon to do so by a member of the WSWG or the facilitation team. Federal resource personnel and outside experts will not participate in WSWG decision making. Federal resource personnel and outside experts will be copied on all WSWG materials, including draft documents.

WSWG Members' Staff and Supporting Organizations

WSWG members may be staffed by individuals from their organizations or by individuals from sponsoring/nominating organizations. Every effort will be made to facilitate WSWG members' participation in the WSWG process by ensuring that staff has access to WSWG materials, including internal draft documents. However, staff are not members of the Working Group. To the extent that staff prepare draft comments or other responses for the WSWG member they support, staff must do so in coordination with and as a representative of the WSWG member; actual comments or responses must be submitted by the WSWG member, not by staff.

Decision Making and Consensus

The WSWG will use a collaborative, problem-solving approach, and strive to reach consensus. Consensus is defined as findings that all can "live with." If the Working Group does not reach consensus on a particular issue, the range of views on the Working Group with respect to that issue will be described. Ranges of views, if necessary, will be described in the text of the Working Group's document and will not be attributed to individual members or interests unless the WSWG reaches consensus on an approach to attribution. Working Group members also will have an opportunity to submit up to three pages of individual, attributed comments. Individual comments will be appended to the Working Group document without modification.

Task Teams

The WSWG may choose to establish Task Teams to work on information gathering and analysis related to specific elements of best security practices, incentives, and measures between meetings of the full WSWG. Task Team members must be WSWG members and Task Team meetings are not open to the public.

Meeting Materials and Summaries and Electronic Communication

As much as possible, meeting agendas and supporting materials will be distributed by the facilitation team at least one week before WSWG meetings and conference calls. After WSWG meetings and conference calls, summaries of key discussion points, tentative areas of agreement, and action items will be prepared by the

facilitation team and provided to Working Group members for review. As much as possible, these summaries will be distributed within two weeks of the meeting or conference call.

All WSWG documentation and correspondence will be distributed to all WSWG members. Electronic communication mechanisms (largely email) will be used to the greatest extent possible to distribute WSWG meeting materials, summaries, and references.

Draft Documents

The WSWG will work with two types of draft documents: (1) WSWG internal drafts and (2) public drafts. It is important to understand that, in general, both types of drafts are public documents, available for public review upon request to the extent provided for under the Freedom of Information Act and other applicable public disclosure laws. The distinction between the two types of drafts documents has to do with when and how they are distributed.

WSWG internal draft documents will be marked "Internal Draft Working Document—Does Not Represent the Consensus of the WSWG." In general, WSWG internal draft documents are draft meeting summaries and discussion materials prepared by the facilitation team for WSWG consideration.

To encourage a full and candid exchange of views among WSWG members, internal draft documents will not be distributed beyond WSWG members and staff, federal partners, identified outside experts, and the facilitation team. Note that internal draft documents are likely subject to further distribution, including distribution to the press, based on requests under the Freedom of Information Act or other applicable public disclosure laws. If such a request is made, the WSWG will be notified.

Public draft documents will be marked "Public Draft Working Document—Does Not Represent the Consensus of the WSWG." Public drafts are draft documents that are discussed during the open sessions of full WSWG meetings and are therefore available to the public at the meeting.

Meeting agendas, final meeting summaries, and presentations made to the WSWG by non-WSWG members are not draft documents.

WSWG Copy List for WSWG Internal Draft Documents

A copy list will be maintained for distribution of WSWG internal draft documents. The list will include WSWG members' staff, federal partners, identified outside experts, and the facilitation team. As described earlier in this document, staff may include individuals from sponsoring/nominating organizations who are specifically identified by a WSWG member as staff to the member. To the extent that staff prepares draft comments or other responses for the WSWG member they support, staff must do so in coordination with and as a representative of the WSWG member; actual comments or responses must be submitted by the WSWG member, not by staff.

The copy list for internal draft documents will be provided to WSWG members, and if individuals are added to or subtracted from the list, the WSWG will be notified.

WSWG Copy List for Non-Draft Documents

A copy list will be maintained for the WSWG for distribution of non-draft documents. This list will include individuals who have requested that they be kept up to date on the WSWG process, and may include members of the press. The copy list for non-draft documents will be provided to WSWG members, and if individuals are added to or subtracted from the list, the WSWG will be notified.

FACA, Open and Closed Meetings, and Public Comment

The WSWG chartering entity, the NDWAC, is a Federal advisory committee established and operating under the requirements of the Federal Advisory Committee Act (FACA). The WSWG is a working group to the NDWAC and is not a Federal advisory committee.

Consistent with the ground rules for Working Groups established by the NDWAC, WSWG meetings will be announced in the *Federal Register*.

In general WSWG meetings will be open to the public for observation and will include an opportunity for members of the public to offer oral and written comments. Meetings and conference calls of the full WSWG that are open to the public will be taped.

The WSWG may decide to close portions of their meetings to the public to provide a forum for discussion of security-sensitive information, as described below.

Security Sensitive Information

The WSWG may have occasion to discuss security-sensitive information. For purposes of WSWG deliberations, the group agrees that security-sensitive information is:

- Information on system-specific, attributable tactical security procedures; or
- Integrated or aggregated detail on security (e.g., by aggregating information from previous un-aggregated sources) that creates a clear picture of a specific strike opportunity.

Information that is already available in the public domain in the same form and at the same level of detail discussed by the WSWG is not security sensitive.

WSWG meetings will be closed to the public as necessary to provide a forum in which WSWG members can discuss potentially sensitive information related to specific security tactics used by individual utilities. As much as possible, closed meeting sessions will be scheduled to be convenient for those attending the portions of WSWG meetings that are open to the public (e.g., they will be at the beginning or end of meetings). During closed meetings, the following protocols will be used.

- The meeting will be open only to WSWG members, federal resource personnel, facilitation support contractors, and identified outside experts.
- The general topics of discussion covered during the closed portion of the meeting will be documented in the meeting summary; discussion details will not be summarized.
- Any meeting materials that are distributed during the closed portion of the meeting will be collected at the end of the meeting unless they are deemed suitable for public disclosure.
- The WSWG will evaluate discussions that occur during a closed meeting at the end of the meeting and determine if any security-sensitive information was discussed that requires protection going forward. The Group agrees that a low threshold for identification of security-sensitive information is appropriate, and that any individual member can distinguish information as security sensitive.
- Members who choose to raise or discuss tactical level security-sensitive information or other integrated security-sensitive information will indicate that they consider the information they are sharing security sensitive. Unless permission is given by the person who shared the security-sensitive information, members will not attribute any information that a fellow member asserts is security sensitive; furthermore, members will not discuss such information outside closed WSWG meetings, provided such information is not already available in the public domain in the same form and at the same level of detail.
- The closed portion of the meeting will not be taped.

The WSWG agrees that to maximize the usability of their Report, they will strive to limit inclusion of security sensitive information in the written materials they consider and produce.

Communications with the Press

Recognizing that the way in which Working Group deliberations are publicly characterized will affect the group's ability to reach consensus, WSWG members and other parties involved in the WSWG process are encouraged to refer inquiries from the press to the facilitation team or to final meeting summaries or other final WSWG materials. Individuals who choose to speak with the press agree to limit remarks to personal views and to refrain from characterizing the views of, or attributing comments to, the full WSWG, other individual members, or the NDWAC.

Schedule

The WSWG will provide a final report of their findings to the NDWAC in time for the Council's spring 2005 meeting. It is anticipated that the Council will meet in May 2005, and that the final WSWG report will be completed and provided to the Council in April 2005. The WSWG will commence with its first conference call on July 6, 2004. It is anticipated that the group will meet in person five times and will meet by conference call four to six times.

ATTACHMENT 3: TRANSMITTAL MEMO

TO: National Drinking Water Advisory Council

FROM: Membership of the NDWAC Water Security Working Group

DATE: May 18, 2005

SUBJECT: Final WSWG Water Sector Security Findings

The Water Security Working Group (WSWG) is pleased to present these final consensus findings to the National Drinking Water Advisory Council (NDWAC).

The WSWG represents a wide range of interests and perspectives on water security. The 16 members of the WSWG include representatives of public and private, small, medium, and large water and wastewater utilities, public health advocates and regulators, and environmental and public health interest organizations. Dr. Rebecca Head of Monroe County Health Department (also a NDWAC member) and David Binning of Fairfax Water ably served the WSWG as co-chairs. In addition to Dr. Head, NDWAC members on the WSWG were John Young of American Water Works Service Company, Inc., and Jack Betkoski of the Connecticut Department of Public Utility Control.

The NDWAC charged us to:

- Identify, compile, and characterize best security practices and policies for drinking water and wastewater utilities and provide an approach for considering and adopting these practices and policies at a utility level;
- Consider mechanisms to provide recognition and incentives that facilitate a broad and receptive response among the water sector to implement these best security practices and policies, and make findings as appropriate; and
- Consider mechanisms to measure the extent of implementation of these best security practices and policies, identify the impediments to their implementation, and make findings as appropriate.

We make 18 findings in response.

<u>Security</u>
Findings 1 through 6 establish a consistent expectation for what constitutes an "active and effective" water security program and identify 14 features that all active and effective security programs should share. Our deliberations emphasized the need for balance between providing the water sector with a more consistent basis for moving forward with security enhancements and avoiding in any way prescribing the specific security countermeasures individual utilities should use. We characterize this balance as focusing on the "what" not the "how" of security and state clearly that, in the realm of security, "one size does not fit all." Findings 7 and 8 address forging closer partnerships between the utility and public health communities and development of practical, affordable contamination surveillance and monitoring technologies.

Incentives

Findings 9 through 15 call on EPA, DHS, state agencies, utility trade associations, and others to create incentives for development and maintenance of security programs. Many incentives involve education, such as education to raise utility awareness about the benefits of security enhancements and the potential liability resulting from a failure to address security, and education to ensure that organizations which influence utility costs and revenues (e.g., rate and fee setting organizations) understand security imperatives. Other incentives involve targeted technical assistance, creation of programs for utility peer-to-peer assistance and review, and support for inclusion of water utilities in security-related planning and exercises. We also appeal to Congress, EPA, and DHS to increase grant and loan funding for water security.

Measures

Findings 16 and 17 address measurement of individual security program progress. We recommend "core" measures for use by all utilities during annual self-assessments of security progress, and we provide an additional suite of sound measures for utilities to consider.

In Finding 18, we propose three areas of sector-wide, national aggregate measurement: (1) progress implementing "active and effective" security programs, as measured by the degree of implementation of the 14 features of active and effective security programs; (2) progress reducing the number of assets identified as a high security risk measured using the results of vulnerability assessments; and (3) progress reducing the inherent risk potential of utility operations measured by Clean Air Act Section 112(r) reporting on hazardous substances and by the number of utilities that convert from use of gaseous chlorine to other forms of chlorine or other treatment methods. Except for the measure based on 112(r) data, we envision national measures will initially rely on a utility self-assessment and request that EPA work with the water sector and stakeholders to explore options for enhancing the consistency and credibility of national measures through peer review, 3rd party verification, blind surveys, or other more independent assessments. To address concerns about the inappropriate release of individual utility security sensitive information, we believe EPA should publish national measures on a strictly aggregated basis and ensure appropriate confidentiality for submitted data.

We forward these findings to you for consideration and approval, and recommend that they be forwarded to EPA for use in support of the national water security program. We invite your attention to the use of these findings by individual water utilities and water security partners. Recommendations addressing each constituency can be readily identified by focusing on the "should" findings throughout the document. Our findings reflect a consensus of the diverse perspectives of the WSWG on important water security program attributes, reached after a systematic effort involving hundreds of hours of work. We hope you will review them in light of this arduous process and the delicate nature of reaching consensus.

The WSWG understands that our work is now over, and that the full Council will review our findings and may make revisions before making recommendations to EPA's Administrator. In previous reports to EPA, the Council has described any substantial revisions it makes to working group findings; if possible, we would very much appreciate if this approach could be used to describe any major revisions you might make to our findings so we can better understand the Council's views.

The WSWG greatly appreciates this opportunity to contribute to water security progress, and we thank you for allowing us to serve. We welcome the NDWAC's review of our work and look forward to your response.

ATTACHMENT 4: ANNOTATED BIBLIOGRAPHY OF SECURITY RESOURCES

American Chemistry Council. *Responsible Care Security Code of Management Practices*. Washington, DC: American Chemistry Council, accessed on-line October 2004. URL: http://www.americanchemistry.com/rc.nsf/7120e6a3c6a45fd8852568d5006a33f4/67f8d93b3af1da8685256ccd005946c8/$FILE/ResponsibleCareSecurityCode.pdf

The ACC outlines the key elements of a security program under the Responsible Care management system. Members of Responsible Care use the code as a set of guidelines as they start implementing and reviewing their own security programs.

American Chemistry Council. *Implementation Guide for Responsible Care Security Code of Management Practices*. Washington, DC: American Chemistry Council, July 2002. URL: http://www.americanchemistry.com/rc.nsf/7120e6a3c6a45fd8852568d5006a33f4/67f8d93b3af1da8685256ccd005946c8/$FILE/Responsible%20Care%20Site%20Security%20Guidance.pdf

This guide provides detailed strategies and examples for implementing the Responsible Care Security Code of Management Practices. It is a resource guide for the Responsible Care companies who are interested in improving the development, management, and planning of their new security programs.

American Chemistry Council. *Responsible Care Management System*. Washington, D.C.: American Chemistry Council, August 15, 2003, accessed on-line October 2004. URL: http://www.americanchemistry.com/rc.nsf/2febeebd340dda4a8525680b004b7f4a/baa1c0d054bf7539852569fc005747c9/$FILE/RCMS%20Technical%20Specification%20-%2008-15-03.pdf

This document is a full explanation of Responsible Care's management systems and guiding principles. It explains the elements of the management system in detail and covers topics that include planning, operations, corrective action, preventative action, management review for chemical companies that are taking part in the program.

American Chemistry Council. Site Security for the U.S. Chemical Industry. American Chemical Council, Chlorine Institute, and the Synthetic Organic Chemical Manufactures Association. October 2001. URL: http://www.cl2.com/SecurityguidanceACC.pdf http://www.accnewsmedia.com/docs/100/89.pdf

This document serves as a general guide for the chemical industry to review general laws concerning security. The American Chemistry Council, the Synthetic Organic Chemical Manufacturers Association, and The Chlorine Institute, Inc. discuss the benefits and steps needed to be taken to develop improved security programs.

American Chemistry Council, Chemtrec, The Chlorine Institute, et al. *Transportation Security Guidelines for the U.S. Chemical Industry*. Additional authors: Compressed Gas Association & the National Association of Chemical Distributors. Washington, DC: 2001.
URL: http://www.accnewsmedia.com/docs/300/250.doc?DocTypeID=4&TrackID=

This set of guidelines covers the benefits of developing a transportation security program, risk-based security assessments, and helpful resources. It targets transportation officials, business managers, plant managers, and others who are responsible for the secure transportation of their chemical supplies and other business materials.

American Society of Chemical Engineers, American Water Works Association, & Water Environment Federation. *Interim Guidelines for Designing an Online Contaminant Monitoring System*. December 9, 2004.

These Guidelines provide information on assessing the need for a contaminant monitoring system, locating instruments and sensors, and responding to suspected contamination events.

American Society of Chemical Engineers, American Water Works Association, & Water Environment Federation. *Interim Voluntary Security Guidance for Water Utilities*. December 9, 2004. URL: http://www.awwa.org/science/wise/

The Guidelines provide advice on security considerations regarding operations, management, design, cyber security management, equipment, and emergency response planning for water utilities seeking to voluntarily improve their security systems.

American Society of Chemical Engineers, American Water Works Association, & Water Environment Federation. *Interim Voluntary Security Guidance for Wastewater/ Stormwater Utilities*. December 9, 2004. URL: http://www.awwa.org/science/wise/

The Guidelines provide advice on security considerations regarding operations, management, design, cyber security management, equipment, and emergency response planning for wastewater and stormwater utilities seeking to voluntarily improve their security systems.

American Water Works Association (AWWA). Emergency Planning for Water Utilities. Denver, CO: AWWA Manual M-19 (Fourth Edition), ISBN: 1-58321-135-7, 2001.
URL (to order on-line): http://www.awwa.org/bookstore/product.cfm?id=30019

This planning guide for water utilities presents principles and practices for emergency planning. The approach focuses on how to apply organizational knowledge and experience within a specific system, determine the system vulnerabilities, address deficiencies, and plan for alternate strategies when needed. It includes sections on hazard summary; vulnerability assessment; mitigation actions; preparedness planning; and emergency response, recovery, and training.

American Water Works Association (AWWA). New Horizons: Critical Infrastructure Protection. Denver, CO: AWWA DVD or VHS Tape, 2001.
URL (to order on-line): http://www.awwa.org/bookstore/product.cfm?id=64226

The goal of this 26-minute video is to generate conversations among water utility managers and selected community leaders about water utility security. It seeks to address the question: "How ready or safe is your water supply to hostile acts of aggression?" The video also discusses infrastructure vulnerability, emergency response plans, contamination, cyber attack, and other intentional acts of destruction.

American Water Works Association Research Foundation & the United States Environmental Protection Agency. Security Practices Primer for Water Utilities. Subject Area: Efficient and Customer Responsive Organization, Denver, CO and Washington, DC, 2004. (DFO) URL (to order): http://www.awwarf.org/research/TopicsAndProjects/execSum/2925.aspx

This primer is an initial assessment of water security for utilities that wish to address pressing security concerns. It covers several topic areas including employee background checks and security training, mail screening, coordination with local medical care providers, and information and communications security.

Association of Drinking Water Administrators & National Rural Water Association. *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems Serving Populations between 3,300 and 10,000.* November 13, 2002. URL (on-line download is free): www.asdwa.org/docs/2002/FINAL10KSystemVAtool111302.pdf

This guide was designed to help drinking water systems serving populations of between 3,300 and 10,000 persons to identify critical components of vulnerability assessments, complete assessments required under the Bioterrorism Act, and identify security measures to be implemented.

Association of Metropolitan Sewage Agencies. Asset Based Vulnerability Checklist for Wastewater Utilities. Washington, DC: 2002. URL (on-line download is free): http://www.amsa-cleanwater.org/pubs/2002avcheck.pdf

The Asset Based Checklist is intended for wastewater managers as a means to evaluate their overall assets, and to subsequently secure and protect their organization based on the evaluation. The checklist breaks assets into five categories: the physical plant, the people (i.e. staff), the knowledge base, the information technology, and the customers. It provides a system for prioritizing risk and includes steps to improve risk management.

Association of Metropolitan Sewage Agencies. Legal Issues in a Time of Crisis Checklist. Washington D.C: 2002. URL (to order on-line): http://secure1.isproductions.net/Merchant2/merchant.mv?Screen=PROD&Store_Code=AMSA&Product_Code=PSECTY02&Category_Code=PSECTY

The *Checklist* is designed to assist wastewater utilities with assessing the legal issues that arise from bioterrorist acts or other crisis situations. It targets public utility attorneys and utility managers who are concerned about crisis management, emergency planning, and response mechanisms, and lays out the possible and detailed steps needed in planning to avoid legal complications.

Bernowsky, Joseph, P.E. Water System Security: A Field Guide. Washington, DC: American Water Works Association (AWWA), ISBN 1-58321-193-4, 2002. URL (to order on-line): http://www.awwa.org/bookstore/product.cfm?id=20501

This field guide provides tools for small and medium sized water utilities to assess vulnerabilities, write emergency plans, review threats, examine mitigation measures, implement new security policies, select and install new technology, and carryout recovery and response from an emergency event. It includes a computer disk with documents and a list of information sources included in the appendix.

Burns, Nicolas L., et al. Security Analysis and Response for Water Utilities. Washington, DC: AWWA, 2001. (Available as a supplement to AWWA Manual M-19).

This concise 20-page guide written in 2001 is now a supplement to *Manual M-19: Emergency Planning for Water Utilities*. M-19 focuses mainly on natural disasters such as earthquakes and severe storms. This guide reviews international acts of terrorism, hazard assessment, vulnerability assessment, crisis communications, mitigation, and development of a response plan in a post 9/11 world.

Blaha, Frank J. *Small System Security-There Is Help And Hope*. American Water Works Association Journal. Denver, CO: Vol.95, Iss. 7; pg. 31, July 2003. Available through Proquest's ABI/INFORM Trade & Industry database.

This article focuses on small and medium sized water utilities that are looking to use the Security Vulnerability Self-assessment Guide for Small Drinking Water Systems Serving Populations between 3,300 and 10,000. The tools addressed were developed as a partnership between NRWA, ASDWA, and the EPA. The article reviews each of the six technical issues or elements outlined by the US EPA.

Booth, Ron, Chuck: Hewell, and Dan Ryan. Technical Security and Countermeasures White Paper for Water Utilities. The National Council for Public-Private Partnerships, Washington, DC: December 12, 2001. URL: http://ncppp.org/inthenews/waterwhitepaper.html

This is a general analysis of measures and damages that water utilities may expect from terrorist threats. The types of threats and damages are analyzed briefly and categorized into four areas: physical damage, damage to chemical storage areas, biological/chemical attack indicators, and cyber terrorism. The paper includes a "Facility Security Survey," which is a detailed checklist of questions for a vulnerability assessment (Appendix A).

Bramwell, Moses J. Champlin Water Works Seeks Right Level of Security Against Terror Threats. Journal of the American Water Works Association (AWWA). Vol. 94(4):54-56. Denver, CO: AWWA, April 2002. Available through Proquest's ABI/INFORM Trade & Industry database.

This article is a case study that examines how a water utility in Champlin, Minnesota worked to improve their security. It reports on the benefits of having a wireless security system, customizing security systems to fit needs and objectives, and educating alarm and security companies as well staff on new security procedures or designs.

Cody, Betsy & Opeland, Claudia. Terrorism and Security Issues Facing the Water Infrastructure Sector. Washington, DC: Congressional Research Service (CRS), Updated May 2003.
URL: http://www.ncseonline.org/NLE/CRS/abstract.cfm?NLEid=39364

This brief report is a legislative analysis of Federal responses to the call for improved security in critical water related infrastructure. It reviews the details of legislation focusing on wastewater utilities (H.R. 866 and S. 1039) and details the various budget proposals for water security improvements until May 2003.

Denileon, Gay Porter. *The Who, What, Why, and How of Counter Terrorism Issues*. American Water Works Association Journal. Denver, CO: Vol. 93, Iss. 5; pg. 78, 8 pgs, May 2001. Available through Proquest's ABI/INFORM Trade & Industry database.

This white paper provides a history of water sector security issues in the late 1990's and before September 11th, 2001. It analyzes the Presidential Decision Directive 63 which established the National Infrastructure Protection Center and looks at how the U.S. EPA became the lead agency on "critical water infrastructure protection issues for the water supply sector." It also includes a checklist of security measures for utilities to consider.

Dyches, Kim. Drinking Water System Emergency Response Guidebook. Utah Department of Environmental Quality, Salt Lake City, UT: November 2002.
http://drinkingwater.utah.gov/documents/compliance/emergency_response_guide.pdf

This guidebook's goal is to help private and public utilities design or prepare a disaster/ emergency response plan. It covers several key areas including organizational structure, implementation, how to prioritize needed repairs, dispatching personnel and equipment, requests for emergency response or aid, and the notification of the public/ how to prepare press releases. It also includes a "Recovery Checklist," which includes steps to recover from a water-related emergency.

Garcia, Mary Lynn. The Design and Evaluation of Physical Protection Systems. Sandia National Laboratories. Butterworth-Heinemann, ISBN: 0750673672, February 2001.
URL: (to order) http://www.campusi.com

This book is a guide to determine the objectives of a security system or program, design the security system in detail, and evaluate the components and performance of the security system. It is targeted

towards security students and professionals in the field. The book includes a sample model for performance analysis of security systems to estimate or evaluate performance against threats.

Gelting, Richard J, PhD, & Miller, Mark D. *Linking Public Health and Water Utilities to Improve Emergency Response*. Southern Illinois University - Carbondale, IL: Journal of Contemporary Water Research & Education, Issue 129 - Water and Homeland Security, October 2004. URL: http://www.ucowr.siu.edu/updates/129/gelting.pdf

This article reviews the necessary connections between medical service providers, water utilities, and public health officials in the case of a bioterrorist water contamination event. The authors state that the link between emergency responder and water utility managers will directly influence the speed and success of a community's response.

Hebert, Robert E., A Brief Discussion of Water Security Issues Following the September 11, 2001 Terrorist Attacks. Washington, DC: The National Council for Public and Private Partnerships, December 12, 2001.
URL: http://ncppp.org/inthenews/waterdiscussion.html

This article discusses threats to the nation's water systems on a general level. It is targeted for an audience of elected officials, city managers, and private utility owners. The author organizes his discussion of security into three categories or "pillars": prevention, detection, and response.

Hickman, Major Donald C. Chemical and Biological Warfare Threat: USAF Water Systems at Risk. *Air University,* Maxwell Air Force Base, AL: September 1999.
URL: http://www.au.af.mil/au/awc/awcgate/cpc-pubs/hickman.htm

The strategy paper examines systems and ideas to identify critical infrastructure points that may be vulnerable to chemical or biological weapons attack. The author reviews four areas to improve security and protection of the USAF water systems: vulnerability assessments, re-evaluation of conventional wisdom on chemical and biological weapons, and a review of how engineering and management of water systems are outsourced by the USAF.

The Homeland Security Council. *Planning Scenarios: Executive Summaries (Created for Use in National, Federal, State, and Local Homeland Security Planning Activities)*. The Homeland Security Council: David Howe, Senior Director for Response and Planning. Washington, DC: July 2004.
URL: http://www.altheim.com/lit/planning_scenarios_exec_summary.html

The Homeland Security Council has developed a list of 15 scenarios that all national, state-level, and local planning officials should use in security and safety program development.

Lancaster-Brooks Khafra, Engineering Consultant. Water Terrorism: An Overview of Water & Wastewater Security Problems and Solutions, Journal of Homeland Security, Northern Virginia: February 2002.
URL: http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=31

In this article, the author reviews measures to defend water utilities from malevolent threats of vandalism and terrorism. The article lists different types of infrastructure that need protection and examines some measures that utilities have adopted for securing them. It also includes a practical list of questions to review in the "Generic Basic Water System Evaluation."

Landers, Jay. Safeguarding Water Utilities. Civil Engineering: The Magazine of the American Society of Civil Engineers. Vol. 72, No. 6, June 2002.

The article draws a basic map of where the thinking on water security is going through mid-2002. The article includes interviews with experts throughout the sector and touches on several key areas of concern including: redundancy in security systems, determining infrastructure needs, and looking at cost

considerations of new methodologies. The article also touches on the differences between a performance-based approach and one based more on compliance.

Mayes Larry W., PhD, PE, PH. (Ed.) Water Supply Systems Security. McGraw-Hill, New York, NY: 2004. URL (to order): http://www.campusi.com

This book is written by a team of security experts and provides broad coverage of security systems for the water sector. Topics include a review of reliability methodologies, modeling methods for early warning systems, frameworks to improve the security of a water system over time, case studies taken from the field, analysis systems for contamination response, safeguards against cyber threats, and specialized systems for remote monitoring and networks.

National Biosolids Partnership. *Elements of an Environmental Management System for Biosolids*. Excerpted chapter (pp.8-15): *Element by Element Requirements*. Alexandria, VA: Final Interim Draft, May 1, 2002.

This chapter excerpted from an NBP guidance document addresses 17 elements which are prudent in developing an effective Environmental Management System.

Schlegel, Julie. *Automated Distribution System Monitoring Supports Water Quality, Streamlines Systems Management, and Fortifies Security*. American Water Works Association Journal. Denver, CO: Vol. 96, Iss.. 1; pg. 44, 3 pgs, January 2004.

In this article, the author discusses the benefits of real time water quality monitoring and its management applications for water utility management. The article briefly reviews how multiple water quality parameters are monitored simultaneously, the ways in which real-time data can improve water utility management, and how distribution monitoring may ameliorate security.

Tiemann, Mary. Safeguarding the Nation's Drinking Water: EPA and Congressional Actions. Washington, DC: Congressional Research Service (CRS), Updated March, 2003.
URL: http://www.ncseonline.org/NLE/CRS/abstract.cfm?NLEid=34419

This CRS report is a general analysis of Federal legislation including the Homeland Security Act of 2002 (the creation of the Department of Homeland Security), the Public Health and Bioterrorism Preparedness Act of 2002, and appropriations for water security activities through March of 2003.

U.S. EPA. Drinking Water Security website. New England Office, Boston, MA: July 2004.
URL: http://www.epa.gov/ne/eco/drinkwater/dw-security.html

The introductory article and collection of links provides sources of information on vulnerability assessment for water utilities. The article summarizes current work and progress on water security in the Northeast EPA Region.

U.S. EPA. Emergency Response Plan Guidance for Small and Medium Community Water Systems to Comply with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Washington DC: U.S. EPA Office of Water, EPA 816-R-04-002, April 2004.
URL:http://www.epa.gov/safewater/watersecurity/pubs/small_medium_ERP_guidance040704.pdf

EPA published this guide for small and medium community water systems (serving populations between 3,301 and 99,999) to assist them in their effort to develop and revise Emergency Response Plans (ERPs). The document is target audience includes "key authorities with critical roles during emergency response or remediation actions from a drinking water contamination threat or incident."

U.S. EPA. *Guarding Against Terrorist and Security Threats: Suggested Measures for Drinking Water Utilities,* Washington DC: Revised August 2004. URL: http://www.dhs.ca.gov/ps/ddwem/homeland/Appendix/AppendixI_%20USEPAthreatlevelgucemarch_%2031.pdf

This threat guide uses the Green, Blue, Yellow, Orange, Red threat levels developed by DHS. It also outlines measures that water utilities should consider at each given threat level.

U.S. EPA. Guidance for Water Utility Response, Recovery, and Remediation Actions for Man-Made and/or Technological Emergencies. Washington, DC: U.S. EPA Office of Water, EPA 810-R-02-001, April 2002. URL: http://www.epa.gov/safewater/watersecurity/pubs/er-guidance.pdf

This guide is purely reactive in nature as it focuses on the steps water utilities must take in response to man-made or technological problems. It includes information on incident types, guidance development, response planning, notification considerations, sample collection, identification, chain of custody (of samples), SCADA intrusions, structural damage resulting from an international act, and notification from health officials.

US EPA. Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Washington, DC: U.S. EPA Office of Water, EPA 810-B-02-001, January 2003.
URL: http://www.epa.gov/safewater/watersecurity/pubs/util-inst.pdf

This document is aimed at water utility managers who have questions about complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. It answers questions as to instructions at a glance, determining the size of the utility, compliance requirements, key dates, and ways in which to submit the information back to EPA.

U.S. EPA. Large Water System Emergency Response Plan Outline: Guidance to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Washington DC: U.S. EPA Office of Water (4601M), EPA 810-F-03-007, July 2003.
URL: http://www.epa.gov/safewater/watersecurity/pubs/erp-long-outline.pdf

This document is similar intent to the previous, but targeted at larger community water systems (CWS). It covers different topics that include emergency planning processes, emergency response plans, identification of alternative water sources, chain of command charts, communications procedures, personnel safety, equipment, property protection, training exercises (or drills), emergency action procedures, incident specific emergency action procedures, next steps, and other references.

U.S. EPA's Drinking Water Academy. Learner's Guide to Security Considerations for Small Drinking Water Systems: Major Security Considerations When Performing a Sanitary Survey of a Small Water System. Washington, DC: U.S. EPA Office of Water, publication EPA 816-R-03-013, August 2003. (DFO)
URL (to order): http://www.epa.gov/OGWDW/dwa/resources.html

The *Learner's Guide* is a tool to be used by community water systems serving fewer than 10,000 people. It was developed as part of a partnership with the Association of State Drinking Water Administrators (ASDWA) and the EPA Drinking Water Academy's Sanitary Survey Workgroup. It examines a multiple barrier approach to security, utility management, water sources, water pumps, the water treatment process, storage facilities, and distribution systems at small water utilities.

U.S. EPA. Response Protocol Toolbox: Planning for and Responding to Contamination Threats to Drinking Water Systems. Washington, D.C.: December 2003 to April 2004. (DFO).
URL: http://www.epa.gov/safewater/watersecurity/pubs/guide_response_overview.pdf

The goal of this EPA Toolbox is to assist water utilities to "effectively and appropriately respond to intentional contamination threats and incidents." It was written and revised by the EPA in partnership with the Metropolitan Water District of Southern California. It targets water utilities, laboratories, emergency responders, state drinking water programs, technical assistance providers, public health and law enforcement officials. It includes an overview and six separate modules (or tools) that can be used independently.

U.S. EPA's Drinking Water Academy, & the National Environmental Training Association. DVD/Video. Security Considerations: Small Water Systems. Are We Ready? Can We Respond? Can We Recover? Washington, D.C.: 2003. (DFO)

A video produced for state and local water systems interested in improving their security programs. The video focuses on key topics in water security. The video is based on EPA's "Learner's Guide to Security Considerations for Small Drinking Water Systems: Major Security Considerations When Performing a Sanitary Survey of a Small Water System."

U.S. EPA. Security Product Guide: Water and Wastewater Security Program Guide. Washington D.C: U.S. EPA website, 2004.
Overview— URL: http://www.epa.gov/safewater/security/guide/index.html
Table of Contents—
URL: http://www.epa.gov/safewater/watersecurity/guide/tableofcontents.html

The web-based guide provides information on products that may help utilities improve physical and cyber security measures. The guide evaluates products that are applicable to improving distribution systems, wastewater collection systems, pumping stations, treatment processes, main plant and remote sites, personnel entry, chemical delivery and storage, SCADA, and control systems for water and wastewater treatment systems.

U.S. EPA. Survey Results on Information Used by Water Utilities to Conduct Vulnerability Assessments. Washington DC: U.S. EPA Office of the Inspector General, Report No. 2004-M-001, January 20, 2004.
URL: http://www.epa.gov/oig/reports/2004/20040120-2004-M-0001.pdf

The survey evaluates the information that some utilities used in the process of writing their vulnerability assessments. It examines the "usefulness of information provided to water utilities by the EPA and others, to discuss other security concerns that water utilities have expressed, and to look at performance indicators that may measure improvements in water security levels or programs."

U.S. EPA. *Table Top Exercise CD ROM: Train-the-Trainer Materials Description* (from trainings organized by the U.S. EPA for the Response Protocol Toolbox). Washington DC: U.S. EPA Office of Water Security, August 2004.

The target audience for this CD ROM is water utility managers and staff as well as their partners in the response community. The goal of the CD is to improve and strengthen the relationships between water utilities and emergency response groups before an incident occurs. The CD includes an introduction, tabletop exercises, and train-the-trainer materials for training workshops (based on the RPTB modules) for printing and distribution.

U.S. EPA. Top Ten List for Small Ground Water Suppliers. Boston, MA: U.S. EPA Northeast Office website, 2004.
URL: http://www.epa.gov/ne/eco/drinkwater/pdfs/drinkingH2Ofactsheet.pdf

This top ten list is a "how to" fact sheet prepared by the EPA's Northeast Office. It allows small water utilities to quickly examine a short list of tasks and actions which will indicate their preparedness for a water related emergency.

U.S. EPA. *Water Security Website*. Washington, DC Office of U.S. EPA: accessed April 2005.
URL: http://cfpub.epa.gov/safewater/watersecurity/index.cfm

This official U.S. EPA water security page provides information on VA's, emergency planning, security enhancements, legislation and directives, trainings, grants, other tools, publications, and related links. It is an important source of materials and information for a water utility manager and interested officials.

U.S. GAO. Report to the Committee on Environment and Public Works, U.S. Senate—Drinking Water: Expert Views on How Future Federal Funding Can Best Be Spent to Improve Security. Washington, DC: GAO-04-29 Drinking Water Security, October 2003. (DFO) URL: http://www.gao.gov/new.items/d0429.pdf

The GAO report reviews the state of water security in a broad manner. The U.S. Senate Environment and Public Works committee commissioned the systematic web based research to discuss water security matters with 43 selected experts. The GAO recommends that the EPA use the report as a guide to allocating funding or resources to water utilities. It outlines the methods it recommends to distribute Federal funding, and a compilation of security-enhancing activities that utilities may undertake.

U.S. GAO. *Testimony Before the Subcommittee on Environment and Hazardous Materials, Committee on Energy and Commerce, House of Representatives—Drinking Water: Experts' Views on How Federal Funding Can Best Be Spent To Improve Security*. Washington, DC: GAO-04-1098T Drinking Water Security, September 30, 2004.
URL: http://www.gao.gov/new.items/d041098t.pdf

U.S. GAO Testimony to follow up on the Report *Senate—Drinking Water: Expert Views on How Future Federal Funding Can Best Be Spent to Improve Security*. This is the most recent discussion of the report before the US Congress (House of Representatives.

U.S. GAO. *Wastewater Facilities: Experts' Views on How Federal Funds Should Be Spent to Improve Security*. Washington, DC: GAO-05-165, January 31, 2005. URL: http://www.gao.gov/new.items/d05165.pdf
Abstract URL: http://www.gao.gov/docsearch/abstract.php?rptno=GAO-05-165
Highlights URL: http://www.gao.gov/highlights/d05165high.pdf

The U.S. GAO summarizes their findings from a web-based survey which involved interviews of 50 experts across the nation to learn more about specific wastewater issues. The issues included: "(1) key security-related vulnerabilities affecting wastewater systems, (2) activities the federal government should support to improve wastewater security, and (3) criteria that should be used to determine how any federal funds are allocated to improve security, and the best methods to distribute these funds."

ATTACHMENT 5: ACRONYM LIST

ACC – American Chemistry Council
ADWA – Association of Drinking Water Administrators
ASCE – American Society of Civil Engineers
AMWA – Association of Metropolitan Water Agencies
AWWA – American Water Works Association
AWWARF – American Water Works Association Research Foundation
Bioterrorism Preparedness and Response Act - Bioterrorism Act
CI – American Chlorine Institute
EPA – The Environmental Protection Agency
ERP – Emergency Response/ Recovery Plan
GAO – Government Accountability Office
HSC – Homeland Security Council
HSIN – Homeland Security Information Network
IT – Information Technology
CDC – Centers for Disease Control and Prevention
DHS – Department of Homeland Security
DoD – Department of Defense
NACWA – National Association of Clean Water Agencies
NBP – National Biosolid Partnership
NDWAC – National Drinking Water Advisory Council
NRWA – National Rural Water Association
NW WARN – NorthWest Warning and Alert Response Network
RAM-W – Risk Assessment Methodology for Water
SCADA – Secure Supervisory Control and Data Acquisition
SEMS – Security and Environmental Management System
V-SAT – Vulnerability Self-Assessment Tool
WaterISAC – The Water Information Sharing and Analysis Center
WEF – Water Environment Federation
WSWG – The Water Security Working Group
WSCC – Water Security Coordination Council