National Drinking Water Advisory Council
Water Security Working Group

August 31 – September 2, 2004 Meeting
Draft Summary

The Water Security Working Group (WSWG) of the National Drinking Water Advisory Council (NDWAC) held its first in-person meeting in Seattle, Washington, August 31–September 2, 2004. Dr. Rebecca Head, the WSWG chair, opened the meeting at 1:30 PM on August 31, 2004 Pacific Daylight Time. The meeting ended at 11:00 AM on September 2, 2004 Pacific Daylight Time. Marc Santora, the designated federal official for the WSWG, was present, as were all WSWG members except for Dave Siburg. Craig Thompson served as an alternate for Mr. Siburg. Tom Forgette was present only for the portion of the WSWG meeting that occurred August 31, 2004. John Laws and Nancy Wong, of the Department of Homeland Security, participated by telephone on August 31, 2004 only. The meeting was facilitated by Rob Greenwood, Ross & Associates Environmental Consulting, Ltd., the support contractor for the WSWG.

The objectives of the first day of the WSWG meeting were to:

- Introduce and welcome WSWG members, federal partners, and resource personnel.
- Review draft WSWG operating procedures and develop a common understanding of the special protocols in place for meeting closure on September 1, 2004.
- Receive information about ongoing federal efforts related to water security and federal roles and responsibilities and begin to develop a common understanding of the role of the WSWG in light of federal efforts.
- Begin to develop a common understanding of utility operations and vulnerabilities, and the current state of security practices.
- Create a common sense of the security-related products the WSWG will produce and capture principles, key considerations, and member needs and interests to inform future security related deliberations.
- Develop a common understanding of the need for, and desirability of, discussion of sensitive security related materials and create a path forward for decisions about closure of, if any, future WSWG meetings.
- Provide an opportunity for public comment.

The portions of the meeting that occurred on August 31, 2004 and September 2, 2004 were open to the public and an opportunity for public comment was provided. The portion of the meeting that occurred on September 1, 2004 was not open to the public to give the WSWG an opportunity to discuss potentially security-sensitive issues.

This document provides a summary of key areas of WSWG discussion, tentative areas of agreement, and next steps. The summary is organized by key discussion topic area, and synthesizes conversations that occurred throughout the three days. The meeting agenda and non-draft meeting materials are available through the WSWG website at http://www.epa.gov/safewater/ndwac/council.html.

The Draft summary of the August 31–September 2, 2004 WSWG Meeting was distributed to the

members of the Working Group for comment, and comments were incorporated. Two changes to the draft meeting summary were made in response to comments. First, "prevention" was added to the discussion of key performance outcomes on the bottom of page 6. (Prevention was discussed in Seattle but accidentally omitted it from the draft summary.) Second, a quote from the Federal Register notice in which the Agency announced formation of the WSWG was added to the discussion Ms. Pawlukiewicz's comments on the use of the word "voluntary" on page 5. The quote expresses EPA's intention to facilitate "the development of voluntary best security practices."

Opening Remarks

Janet Pawlukiewicz, acting director of the EPA Water Security Division, welcomed the WSWG members and thanked them for their service. Ms. Pawlukiewicz emphasized the importance, in EPA's eyes, of the Group working together to help the water sector make security a part of every-day business. She reiterated and expressed EPA's support for the three areas of the WSWG's mission from the National Drinking Water Advisory Council (NDWAC):

- Develop principles and/or general policies and practices for what constitutes an effective security program;
- Identify incentives (and/or barriers) to implementation of such programs; and,
- Identify recognition mechanisms and other measures of program adoption.

Ms. Pawlukiewicz explained EPA's hope that recommendations based on the WSWG's work would help to establish clearer expectations about security programs, and that such expectations would better enable government agencies and utility owners/operators to secure funding for security enhancements. Ms. Pawlukiewicz indicated that EPA is very much looking forward to the outcomes of the WSWG's deliberations and that the Agency is committed to careful consideration of these outcomes and to providing tools, training, and other appropriate support to utilities to help them implement recommendations that may emerge.

Following Ms. Pawlukiewicz's remarks Marc Santora the Designated Federal Officer (DFO) for the WSWG introduced himself and explained that his role is to support the WSWG and act as a resource for the Group throughout its deliberations.

WSWG Draft Operating Procedures and Identifying a WSWG Co-Chair

The WSWG discussed their draft operating procedures and the process of identifying a co-chair on August 31, 2004. Rob Greenwood, of Ross & Associates Environmental Consulting, Ltd., briefly reviewed the draft WSWG operating procedures. Mr. Greenwood highlighted a number of aspects of the operating procedures, including those related to use of alternates, decision making and consensus, and focusing discussions using the needs and interests of WSWG members.

A WSWG member asked about the operating procedures on the role of the chair, and in particular, how the responsibility for reporting to the NDWAC would be determined. The Group discussed the idea that members of the WSWG who are also members of the NDWAC likely will offer informal updates on Group progress during NDWAC meetings, but that formal responsibility for reporting to the NDWAC on the outcomes of the WSWG process would be determined by the Working Group. This point will be clarified in the next revision to the WSWG operating procedures.

Mr. Greenwood reviewed the decision to identify a WSWG co-chair to serve with Rebecca Head. Mr. Greenwood asked that WSWG members provide any suggestions about who should serve as a co-chair to the facilitation team by Friday, September 3, 2004.

Discussion of How FOIA and FACA Apply to the WSWG

The WSWG discussed the Freedom of Information Act (FOIA) and the Federal Advisory Committee Act (FACA) on August 31, 2004. Mr. Santora explained that as a Working Group to a federal advisory committee, the WSWG is encouraged to design a process that is open to public input, but that the Group is not, in its own right, considered a committee chartered under FACA. Mr. Santora further explained that, therefore, as necessary, WSWG meetings can be closed to the public without going through the procedures that might be necessary to close a meeting of a chartered federal advisory committee.

WSWG members asked Mr. Santora if there was the ability to close NDWAC meetings, if necessary, so that the NDWAC could receive and be briefed on the WSWG's report. Mr. Santora explained that there are procedures that can be used to close federal advisory committee meetings to the public, consistent with the requirements and limitations in the Government in the Sunshine Act.

WSWG members asked Mr. Santora about the extent to which WSWG materials were releasable under FOIA. Mr. Santora explained that the analysis under FOIA was more complicated. It appears likely that any documents provided by the WSWG to EPA or to NDWAC, and documents provided by EPA or the EPA contractor to the WSWG, will likely be subject to release under FOIA, except to the extent they are covered by an exemption to FOIA. FOIA exemptions that might be explored include the exemptions for confidential business information and deliberative processes, and exemptions, or protections for security-sensitive information that may flow from the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. Documents that are used only during a closed part of a WSWG meeting and collected at the end of the meeting are not considered "records" under the Federal Records Act, and are therefore not subject to FOIA.

Ongoing Federal Efforts and Federal Roles and Responsibilities

The WSWG discussed federal efforts, roles, and responsibilities on August 31, 2004. Janet Pawlukiewicz gave a presentation on federal roles in water security. Ms. Pawlukiewicz described the federal authorities that apply (including homeland security presidential directives), discussed the ongoing development of National Infrastructure Protection Program (NIPP) measures, and expressed EPA's perspective on the mission of the WSWG. Ms. Pawlukiewicz explained that, in EPA's view, the key outcomes hoped for from the WSWG are: a basic definition of effective utility security programs, to garner support for work needed and show that the sector is taking security seriously; recommendations on actions that EPA might take to support water utilities; and recommendations on mechanisms for NIPP measures. Ms. Pawlukiewicz's presentation is included as Attachment D.

John Laws was scheduled to make a presentation for the Department of Homeland Security (DHS) Information, Analysis, and Infrastructure Protection Directorate. Mr. Laws was unable to travel to the WSWG meeting in Seattle so Ms. Pawlukiewicz presented Mr. Laws' materials, and Mr. Laws, with Nancy Wong, also of DHS, answered questions by telephone. Mr. Laws' presentation materials elaborated on the importance of sector coordinating councils, described the formation of a sector coordinating council for water and wastewater utilities, and compared

the utility sector coordinating council to the WSWG. Mr. Laws' presentation is included as Attachment E.

The WSWG discussed federal roles and responsibilities related to water security, in particular, the differences between the WSWG mission and the role of the water sector coordinating council. In general, the Group was comfortable with the distinction that the water sector coordinating council is a group of more limited participation (it is utility owner/operator only) and is focused on coordination among utilities and operations in the sector, while the WSWG is a group of more broad participation (including utilities and other interests) and is focused on providing recommendations to the NDWAC (and through the NDWAC to EPA) about security practices, incentives, and measures. The Group agreed that in moving forward it will be critical for WSWG activities to be coordinated with the activities of the water sector coordinating council and for attention to be paid to ensuring that the additional work/role of each group is sufficiently unique that each group adds independent value. EPA and DHS agreed to provide additional, written information about the roles of the two agencies and potential coordination between the WSWG and the water sector coordinating council.

The WSWG discussed sequencing of the three areas of its mission, and generally converged around the idea that while all three areas would inform one another, it would be useful to begin with security practices and then to move through incentives and measures. The Group discussed measures, in particular. Ms. Pawlukiewicz clarified that the elements for NIPP measures listed on slide 7 of her presentation are largely put in place as standard reporting categories for each infrastructure element and that EPA's hope is that the WSWG can consider these reporting categories and make recommendations for specific measurement mechanisms.

Tim Mukoda, of the Air Force Medical Support Agency, talked about the Department of Defense's (DoD) role in water security. Major Mukoda talked about two primary roles; first, DoD is interested in participating in any development of principles or policies that may, at a later date, be formally or informally applied to the Department's operations; second, DoD has recent and historical experience with water security through its operation of numerous water plants on secure installations throughout the world and can offer that experience to the group. Major Mukoda discussed, in particular, DoD's recent experience carrying out vulnerability assessments for approximately 200 installations. Major Mukoda's presentation is included as Attachment E.

WSWG Products—Scope and Key Areas for Recommendations

The WSWG discussed the items they might produce on September 1 and 2, 2004.

The WSWG converged around the idea that the scope of their deliberations and products on security should include protection of: public health, public safety (including infrastructure protection), and the ability of the water sector to establish, maintain, and, if necessary, restore public confidence. With respect to public confidence in particular, WSWG members discussed the fact that events that do not present widespread public health or safety risks nonetheless have the potential to dramatically affect public confidence and that a lack of public confidence can cripple a water system.

The WSWG deliberated extensively on the level of detail that their security-related products should involve. From these deliberations, members converged around a level of detail that is focused on security principles as well as security program elements and their implications and application. Members agreed that they would strive to avoid including information on specific security tactics. This was discussed as focusing on the "what to do" not the "how to do it."

From these deliberations the WSWG considered three objectives for their recommendations:

(1) Establish a security practices framework that helps utilities and their key partners assess and prioritize security enhancements to prevent, mitigate, or be better prepared to respond to events that could cause serious consequences.

(2) Motivate utilities to *(voluntarily)* adopt the security practices framework.

(3) Enable utilities to demonstrate security-related need and performance to themselves and their crucial information customers through clear, effective mechanisms to measure preparedness and implementation of security enhancements.

Members converged around objectives (1) and (3) and the broad outlines of objective (2), but did not converge around the use of the word "voluntarily," and there was a diversity of views among members about continuing to use the word "voluntary."

Members interpreted voluntary to mean different things. Some thought it "watered down" the message. Others members expressed a preference for the word voluntary to make it clear that regulatory standards are not desirable. Still other members supported consideration of regulatory approaches and therefore preferred that the word voluntary be removed. After discussion, the Group converged around the idea that there are many ways that a utility might be motivated to adopt a security program framework, and that further deliberation on the many ways to motivate utilities is necessary before the Group can make a decision about use of the word voluntary. Many members suggested that motivation should be as strong as possible, stopping just short of regulations. There was broad agreement in the Group that the intent and desired outcome was to motivate broad and receptive response to the security practices framework, and broad adoption throughout the water sector. Ms. Pawlukiewicz reiterated that EPA is not planning a regulatory effort around water security practices, but instead is looking for mechanisms that provide recognition and incentives for broad and receptive response among the water sector to implement best security practices and policies. This point was also made by the Agency when it announced formation of the WSWG, where the Agency expressed its intention to facilitate "the development of voluntary best security practices."

In addition to objectives for their recommendations, WSWG members converged around a number of key considerations that should be used to guide product development. These key considerations are:

- Don't reinvent the wheel, understand and use existing information, adding new value.
- Limit inclusion of security-sensitive information to maximize the utility of the product and ensure it can be distributed and used.
- Be attentive to concerns that more clearly defining security practices may create liability concerns, especially for smaller utilities that may not have the resources to implement all security enhancements immediately.
- 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.
- It is critical to 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.
- Recognize constraints and barriers but do not be constrained by them, so that, for example, where a practice is desirable but implementation is constrained, recommendations could call for the practice and recognize and recommend ways to overcome constraints. As an example of this situation the WSWG discussed programs for mandatory drug testing of

employees. In some jurisdictions there programs may be difficult to implement because of legal constraints; however, the Group agreed that if these programs are desirable, they should be recommended, and the potential constraints and ways to overcome the constraints should be discussed.
- Products should recognize and address prevention and inherently safer practices as key aspects of enhancing security.
- Products and deliberations should create transparency in decision analysis

The Group agreed that Ross & Associates will develop draft narrative text on product objectives and key considerations for the WSWG to consider during the October meeting.

Recommendation Area 1

Recommendation area 1 has to do with establishing a security program framework. The WSWG discussed three questions that might be used to frame further analysis and draft recommendations on a security framework:

- What is the scope of a security program framework?
- What are the elements of an active and effective security program?
- What context is needed for each program element?

With respect to the scope of a security program framework, as discussed above, the WSWG converged around the idea that the endpoints of an active and effective security program should achieve the protection of public health, public safety, and public confidence. The WSWG also discussed the major consequences that should be addressed by an active and effective security program. The Group converged around the idea that the major consequences to consider for water are: loss of pressurized water for a significant part of the system, long-term loss of supply, treatment, or distribution, catastrophic release of on-site hazardous chemicals affecting public health, and adverse impacts to public health or confidence resulting from a contamination threat or incident. For waste water, the Group converged around the idea that the major consequences to consider are: inappropriate use of the collection system to deliver hazardous materials or devices and long-term loss of treatment capacity resulting from residuals from a contamination or explosive incident.

Finally, the WSWG discussed the need to develop overarching principles of an active and effective security program, such as the principles of coordination, communication and cultural change. The Group agreed that a task team will be formed to further explore the security program framework and develop materials for the full WSWG to consider at the October meeting.

With respect to the elements of an active and effective security program, the Group discussed many potential program elements, such as vulnerability assessments, counter measures enhancements and plans, response action plans, and business continuity plans.

With respect to the context for program elements, the WSWG discussed a number of context features that might be necessary to inform implementation of program elements. For ease of discussion, these features were organized under five broad sub questions. First, how does each program element support key performance outcomes? The key performance outcomes discussed included prevention, preparedness (planning and exercises), response, consequence management, mitigation, and recovery.

Second, what factors inform tailoring of each program element? WSWG members feel strongly

the need to tailor security practices to utility-specific conditions. The Group discussed two types of utility-specific characteristics that might inform tailoring: characteristics that are connected to the inherent "risky-ness" of any given utility's situation, such as whether there is one or multiple sources of source water; and, characteristics that are connected to implementation challenges, such as whether a utility is large or small, or urban or rural.

Third, what are critical success factors for implementation of each program element? The Group discussed factors such as establishing a strong security culture and dedicated leadership attention and commitment to security as examples that might be critical for success. (Note these types of factors were also discussed as potential principles of an active and effective security program.)

Fourth, what are the implementation considerations for each program element? Potential implementation considerations discussed include cost-effectiveness, resource and other requirements for successful implementation, public and political support, legal barriers, and the need to balance potentially-competing implementation priorities in the event of an incident, such as balancing evidence collection needs with recovery needs during incident response.

Fifth, what are key tactical resources for each program element? The Group discussed this as an opportunity to bring forward references to more tactical-level security information that likely would not be covered in detail in the WSWG products because of their security-sensitive nature, but would potentially be useful to utility operators in their design and implementation of a utility-specific security program.

The Group agreed that a task team will be formed to further explore the security program elements and element context and develop materials for the full WSWG to consider at the October meeting.

Recommendation Areas 2 and 3

Recommendation area 2 has to do with motivating utilities to implement the security framework. The WSWG discussed a number of questions that could be used to frame further analysis and draft recommendations on motivating implementation:

- What are the current barriers to implementation?
- How can these barriers be overcome?
- Besides eliminating barriers, what are other mechanisms that may provide motivation?

Recommendation area 3 addresses utilities' ability to demonstrate their individual security performance and the need for security enhancements to themselves and to their critical information customers through clear, effective mechanisms to measure security-related preparedness and implementation. The WSWG discussed a number of questions that could be used to frame further analysis and draft recommendations for measurement mechanisms:

- What key audiences need to understand security-related needs and performance? The WSWG discussed a number of possible key audiences, including ratepayers, utility boards or councils, and government.
- What critical information does each audience need?
- How is information on performance most effectively collected and best assessed and communicated? The Group discussed a number of aspects to this question, including the idea of considering information needs in light of existing databases and data collection, and considering what each audience might experience as the most credible sources of

information (e.g., self-assessments or analysis by an independent body).

Consistent with the sequencing of issues in the draft WSWG Project Plan, the Group agreed that recommendation areas 2 and 3 are largely "on hold" until further progress is made in deliberations on the security program framework (recommendation area 1). Additional briefing materials on recommendation areas 2 and 3 will be discussed during the second meeting of the WSWG, and detailed deliberations likely will begin with the third meeting.

Closure of WSWG Meetings to the Public and Security-Sensitive Information

The WSWG discussed meeting closure and security-sensitive information on August 31, September 1, and September 2, 2004.

WSWG members discussed the definition of security-sensitive information and the use of such information in their deliberations. A number of WSWG members expressed support for, and experience with, open public processes. At the same time, these, and other WSWG members expressed reluctance to reveal any system-specific, attributable, tactical security information in a way that might make such information accessible to individuals or organizations that would seek to do harm. Some WSWG members expressed the view that system-specific tactical details are not what they would anticipate in a report dealing with principles or practices for effective security programs. Members talked about the potential to discuss such information in the context of a closed meeting as exemplifying reasons for, or illustrating, security principles or practices, but not carry forward that type of detail into written materials.

Some members observed that there is a considerable amount of general information about vulnerabilities in the water sector and potential security priorities already in the public domain, and expressed the view that the Working Group likely would not be well served by attempting to keep confidential the types of general information that are already public. Members cautioned against creating any additional security risk or sensitivity by aggregating or compiling information from disparate sources. During deliberations during the closed portion of the WSWG meeting on September 1, 2004, WSWG members discussed, as examples, a number of attributable, utility-specific security tactics.

Tim Mukoda offered a perspective based on the experiences of the US Military. Major Mukoda explained that, in general, unless there are well defined, clear rules for distinguishing security-sensitive information and a person who is responsible for making judgments as to which information is sensitive implementation, will be very difficult. Major Mukoda offered that the DoD model is to declassify as much as possible, because once information is classified its application and usability is limited. Major Mukoda offered to provide further information on DoD classification principles and experience.

In the context of these discussions, WSWG members identified the following attributes of security-sensitive information:

- Information on system-specific, attributable tactical security procedures
- Integrated or aggregated detail on security that creates a clear picture of a specific strike opportunity

Members acknowledged that there likely would remain a range of perspectives on the Working Group about when a document or discussion manifested one or more of these attributes. In particular, some members remained concerned that integrating or aggregating information that is already publicly available, of itself, may cause the information to be security-sensitive;

instead, these members took the view that whether integrated or aggregated public information is security-sensitive would depend on the information and the level of detail or specificity involved. This concern is exacerbated by the fact that, because expanded efforts related to water security are relatively new (although certain types of information e.g., vulnerability assessments have security standards), there is no clear, encompassing baseline establishing what information about security is public and what should remain restricted. Members discussed that, even though some would prefer otherwise, there is already a significant amount of security-related information in the public domain, some of it quite detailed.

From this discussion, members agreed that clarity about when an individual was raising what he or she considered to be security-sensitive information was very important. Members agreed that they would not to attribute any information that a fellow member asserts is security-sensitive. Members further agreed that they would 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. In general members were very comfortable with the idea of not revealing or attributing tactical level security related information. This was referred to as a "confidentiality pact" among the members.

WSWG members agreed that, to maximize the usability of their products, they would strive to limit inclusion of sensitive information. At the same time, the Group acknowledged that portions of their deliberations were enhanced by discussion of security-sensitive information as examples to illustrated concepts, principles or other points.

WSWG members further agreed that future meeting agendas will include closed sessions for sharing of tactical level security experiences/examples, and that other future agenda topics will be evaluated to see if they warrant discussion in a closed session. As much as possible, closed sessions will be structured to be convenient for those attending the portions of WSWG meetings that are open to the public.

The WSWG discussed using the following protocols during closed meetings:

- Meetings will be open only to WSWG members, federal resource personnel, facilitation support contractors, and identified outside experts.
- The general topics of discussion covered during a closed 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 the WSWG decides the materials are 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.
- Members who choose to raise or discuss tactical-level, security-sensitive information will indicate that they consider the information they are sharing security-sensitive. Members will not attribute any information that a fellow member asserts is security-sensitive; furthermore, members will not to 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.
- Closed meetings will not be taped.

Members discussed the need for a written non-disclosure agreement. Some members were interested in a non-disclosure agreement as a ratification of the protocols for closed meetings. Other members expressed concern that because the WSWG deliberations move between sensitive and non-sensitive security information, a non-disclosure agreement would be difficult

to interpret or enforce. Other members expressed the concern that because they are part of a public agency, their ability to sign a non-disclosure agreement may be limited. This issue was not resolved. As a first step, the WSWG agreed to document the attributes of security-sensitive information and the closed meeting protocols to which they have agreed.

Ms. Pawlukiewicz expressed EPA's preference that the WSWG create a report that contains substantive, meaningful recommendations but that is not so sensitive from a security standpoint that access to it must be restricted. Among other things, any need for such restrictions to access could impair the Agency's ability to rely on the report to create tools, training, or other materials to assist utility owners/operators in improving security, diminish stakeholders' ability to rely on a report to support funding and implementation of security enhancements, and limit the usefulness of the report to the sector as a whole. However, Ms. Pawlukiewicz and Mr. Santora also expressed the Agency's willingness to support the WSWG in creating a climate in which they can have meaningful deliberations unencumbered by concerns about revealing security-sensitive information.

September 1, 2004 Presentations to the WSWG

On September 1, 2004, the WSWG considered four presentations. Steve Allgeier, EPA Water Security Division, gave a presentation on the general features of water and wastewater utility operations and vulnerabilities. At a general level, Mr. Allgeier discussed consequences of concern, potential physical, chemical or cyber attacks on water systems, and the use of physical security, early warning systems, and response planning to reduce vulnerabilities.

Rob Greenwood, Ross & Associates, gave a presentation summarizing the ongoing literature review of existing material on utility threats and counter measures, security program elements and principles, and key security outcomes.

Judith Cross, Executive Director of the Seattle Police Department Emergency Preparedness Bureau, gave a presentation on using culture, coordination, and communication as the cornerstones of Seattle Public Utility's water security program.

Upon consideration, and in consultation with the presenters, the WSWG determined that these presentations did not contain security-sensitive information. They are included as attachments F, G, and H, respectively.

In addition, in response to WSWG questions, Fred Light, EPA Inspector General (IG), provided information on the IG's past and ongoing efforts to evaluate water security and the IG's interest in the WSWG. By mutual agreement, Mr. Light did not otherwise attend the closed portions of the WSWG meeting. Mr. Light agreed to provide additional written information on the IG's past and ongoing efforts related to water security.

Distribution of Non-Security Sensitive, Draft Documents

The WSWG discussed protocols for distribution of draft documents that are not security-sensitive. Some members expressed concern, in particular, that the list of interested individuals routinely copied on WSWG materials includes members of the press. The Group discussed that any draft documents provided to EPA likely would be subject to release under FOIA except to the extent that a FOIA exemption, such as the confidential business information, might apply. At the same time, a number of individuals were opposed to the wide distribution of draft documents that currently takes place. To address this concern, WSWG members agreed to review the list of individuals who are routinely copied on WSWG documents and make

suggestions that would focus the list more narrowly on federal partners, outside experts, and staff and supporting organizations for WSWG members.

Tom Forgette's Resignation from the WSWG

Mr. Forgette has resigned from the WSWG due to competing obligations. EPA invited WSWG members to suggest individuals who might be considered as potential replacements for Mr. Forgette. It would be helpful if these individuals, like Mr. Forgette, have emergency preparedness experience from a utility perspective. Some WSWG members suggested that EPA also consider the need for the WSWG to consider the views of the emergency response community (i.e., of responders) in their deliberations.

Public Comment

No individuals offered public comment at the WSWG meetings. One organization, the National Rural Water Association, provided written comments, which are included as attachment J.

Meeting Wrap-Up and Next Steps

As the meeting was drawing to a close, Dr. Head thanked WSWG members for their attention and participation. On behalf of EPA, Janet Pawlukiewicz, acting Director of the EPA Water Security Division, also thanked WSWG members for their attention and their service.

The following action items and next steps were identified during the meeting:

- EPA and DHS will provide additional written material on Agency roles and responsibilities.
- Fred Light, EPA IG, will provide written materials on the IG's past and ongoing efforts related to water security.
- Ross & Associates will circulate additional information on WSWG task teams; WSWG members will volunteer for task teams. Task teams will meet to prepare information on recommendation area 1 for consideration by the full WSWG at the Group's next meeting.
- Ross & Associates will circulate additional information on the needs and interests EPA would like to be represented by Tom Forgette's seat; WSWG members will recommend individuals for EPA's consideration.
- WSWG members will make suggestions for the WSWG co-chair by Friday, September 3, 2004 and the co-chair will be identified by WSWG members using the weight of preferences model.
- WSWG members will review the list of individuals who are copied on WSWG materials and recommend deletions or additions.
- Ross & Associates will revise the draft WSWG operating procedures to capture the protocols for closed meetings and WSWG members will review the revised draft operating procedures.
- In addition to the agenda topics identified in the draft WSWG high-level project plan, the agenda for the next in-person WSWG meeting will include: (1) a significant amount of time that will be closed to the public to allow WSWG members to discuss additional examples of tactical-level security approaches; (2) discussion of task team work on a security program framework and security program elements and context; and (3) initial discussions on recommendation areas 2 and 3, incentives and measures, respectively.

Attachments

Meeting Materials—Non-Draft Documents

Attachment A: Meeting Agenda
Attachment B: NDWAC Working Group Ground Rules
Attachment C: Presentation of Janet Pawlukiewicz, dated August 31, 2004
Attachment D: Presentation of John Laws, dated August 31, 2004
Attachment E: Presentation of Tim Mukoda, dated August 31, 2004
Attachment F: Presentation of Steve Allgeier, dated September 1, 2004
Attachment G: Presentation of Rob Greenwood, dated September 1, 2004
Attachment H: Presentation of Judith Cross, dated September 1, 2004
Attachment I: Comments from National Rural Water Association, dated August 31, 2004

Meeting Attendance and Participation
Attachment J: WSWG Roster and Contact List
Attachment K: List of Members of the Public and Technical Resource Personnel in Attendance

Additional Meeting Materials—Draft Documents, Not Attached
- WSWG Revised Draft Operating Procedures, dated August 18, 2004
- Draft annotated bibliography of security-related resources, dated August 31, 2004
- WSWG Draft Project Plan (including proposed schedule of meetings), dated August 18, 2004
- American Society of Civil Engineers draft materials on physical security practices, three documents, distributed on CD