National Drinking Water Advisory Council
Water Security Working Group

October 27 – 29, 2004 Meeting Summary

The Water Security Working Group (WSWG) of the National Drinking Water Advisory Council (NDWAC) held its second in-person meeting in Washington, D.C., October 27 – 29, 2004. Mr. David Binning and Dr. Rebecca Head, the WSWG co-chairs, opened the meeting at 12:30 PM EDT on October 27, 2004. The meeting ended at 1:15 PM EDT on October 29, 2004. Marc Santora, the designated federal officer for the WSWG for the Environmental Protection Agency (EPA), was present, as were all WSWG members. Paul Bennett, of the New York City Department of Environmental Protection, replaced Tom Forgette. Mr. Forgette has resigned from the WSWG because of schedule conflicts.

Federal partners present were EPA (Janet Pawlukiewicz, David Travers, and Debbie Newberry), the Centers for Disease Control (Mark Miller), and the Department of Homeland Security (John Laws). Jasper Welsch from the Mississippi Department of Emergency Management was present as an identified outside expert to the WSWG. The meeting was facilitated by Rob Greenwood and Elizabeth McManus, Ross & Associates Environmental Consulting, Ltd. (Ross & Associates), the support contractor for the WSWG.

The WSWG had seven objectives for their October meeting.

- Gather and share information on security program approaches, incentives, and measures.
- Share tactical-level security experiences in key security program areas.
- Converge around a framework for describing an active and effective security program, and a set of program features to support development of draft recommendations.
- Understand member needs and interests around incentives for broad adoption of security practices, and develop an approach to WSWG products on incentives.
- Finalize the WSWG operating procedures.
- Confirm the WSWG project plan, and discuss research and speaker needs for future WSWG meetings.
- Provide an opportunity for public comment.

Except for lunch time on October 28, 2004, the portions of the meeting that occurred on October 28 and 29, 2004 were open to the public, and opportunities for public comment were provided. The portions of the meeting that occurred on October 27, 2004 and October 28, 2004 from approximately 12:00 – 1:15pm were 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.

A draft of this document was distributed to the WSWG for comment, and comments were incorporated. Changes made in response to comments from WSWG members:

- clarified (in the list of considerations to inform WSWG deliberations) the need to recognize and manage the relationship between practices that increase safety and those that increase security;
- clarified the description of the WSWG discussion of the scope of an active and effective security program, particularly the discussion of prevention of mortality, protection of the environment, and avoidance of adverse economic consequences;
- added reducing legal liability, and better bond or insurance ratings to the list of potential incentives for adoption of active and effective security programs (these were discussed during the meeting and were included in the list of possible benefits of an active and effective security program but were inadvertently omitted from the summary of possible program incentives);
- clarified that there is no plan for the WSWG to receive information that is legally restricted under the Bioterrorism Act; and,
- fixed typos.

Scope, Principles, and Features of an Active and Effective Security Program

The WSWG considered the work of two task teams that worked between the first and second WSWG meetings to further define and describe an "active and effective" security program. Task teams developed materials that described: WSWG deliberations on security and key themes in security-related deliberations; the scope of an active and effective security program; program goals, objectives, and principles; program dimensions; and program features and how to organize and describe program features.

Description of WSWG Deliberations and Key Themes

The Group converged around ten key considerations that should inform WSWG deliberations on an active and effective security program. These revise the considerations discussed at the Seattle WSWG meeting and described in the Task Team A materials, and are as follows.

- 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. 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.
- Products should recognize and address prevention as a key aspect of enhancing security.
- Products should recognize that inherently safer practices, or practices that have a lower risk potential, also have potential to enhance security.
- 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 might create a safety barrier to an emergency exit.

- Products and deliberations should be developed in a transparent way, and should encourage transparency in individual utilities' security-related decisions.

The Group discussed in particular the idea of considering the potential to create liability concerns by having clearer definitions. The Group had a range of views about how much of a concern the potential to create liability was. Some members were not overly concerned, believing that the level of detail that the Group was considering in its recommendations was not so specific as to create a liability standard. And, in any case, this concern could be easily managed through the Group's commitment to tailor any active and effective security program described by the WSWG to be appropriate for specific systems (including small systems). Others were more concerned. The Group reiterated its commitment to move away from "best security practices," which might imply a specific model for all utilities regardless of their circumstances, and move toward defining an "active and effective" security program, which could then be tailored to the needs of individual utilities.

The Group was very comfortable with the idea that while the same framework and analysis might apply across the water utility sector, the details of any individual utility's security program will be utility-specific and will vary among utilities, based on their specific circumstances. This was discussed as describing "what to do" rather than "how to do it." The Group was comfortable with continuing to include the issue of liability as a consideration, provided other considerations also are included.

The Group also discussed creation of transparency in decision analysis—both in the sense of how the WSWG develops its recommendations and how any individual utility might tailor a security program—as being an important factor in promoting "buy in" and implementation.

The WSWG also discussed and converged around key themes that are emerging from deliberations on security practices. Four key themes have been identified to date, and additional themes may be identified (and these themes revised and refined) as deliberations continue. Key themes identified to date are:

- one size does not fit all;
- programs should have measurable goals and timelines;
- continual improvement is important; and,
- 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.

The Group agreed that a description of the WSWG deliberations including key considerations and emerging themes should be developed into draft report text for further consideration.

Program Scope

The WSWG continues to converge around the idea that the scope of an active and effective security program should be to make efforts to protect public health, public safety (including infrastructure), and public confidence. The Group discussed three refinements to the discussion of the scope of an active and effective security program.

First, the Group discussed the need to include in any discussion of protection of public health and safety the idea that prevention or minimization of death (whether as a direct consequence of water consumption or from the lack of water pressure or volume to fight fires or respond to other events) is one of the results of such protection. The Group also discussed and was comfortable with the idea that the public health community deals with mortality rates and the overall health of communities, rather that individual mortality.

Second, the Group talked about protection of the environment, both in the sense of preventing adverse environmental outcomes that might result from a significant system failure and in the sense of protection of the quality of source water for some utilities. The Group recognized that different utilities, because of their specific circumstances, will have varying levels of concern about environmental protection.

Third, the Group discussed avoidance of adverse economic consequences that could result from a significant system failure. There was strong interest in mentioning avoidance of adverse economic consequences (for example, as a result of having to close beaches because of sewerage overflow) should be discussed as one of the benefits of an active and effective security program.

After discussing program scope, the Group discussed the potential consequences and key threats that active and effective security programs should consider. Consequences are adverse outcomes that might disrupt or endanger public health, safety, or confidence; or might disrupt or endanger the environment or economic vitality. The Group is now considering seven consequences of concern, which revise the consequences of concern discussed at the Seattle WSWG meeting and described in the Task Team A materials.

- 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.
- Adverse impacts to public health or confidence resulting from a contamination threat or incident.
- Long-term loss of collection capacity.
- Long-term loss of treatment capacity.
- Use of the collection system as a means of attack on other targets.

The Group discussed the need to frame the consequences of concern as broad outcomes, rather than try to list with any specificity any of the myriad events that might, individually or in combination, cause or contribute to one or more of the consequences. The Group also discussed the need to use language that is broad enough to be relevant to all utilities, and to emphasize the need for individual utilities to prioritize their efforts to address the consequences and threats that are most concerning and most relevant to their specific circumstances.

Threats are categories of types of attack that, depending on their nature and success, could have the potential to bring about one or more of the consequences of concern. The Group is considering four principle threats.

- Physical targeting of core facilities or interdependent infrastructure, including power and transportation.
- Chemical or biological material used to contaminate water supplies or infrastructure.

- Cyber attack on information technology assets to disrupt service and/or obtain confidential information.
- Use of conveyance tunnels to stage attack against utilities or other targets.

In the summary of the Seattle WSWG meeting and the Task Team A materials, consequences of concern are described as "major" consequences to "consider and protect against." The Group was not comfortable with continued use of the word "major" to describe consequences, since this seemed to involve too much of a subjective evaluation on the part of readers. Instead, the Group discussed "consequences of concern" or simply "consequences." The Group also discussed the need to clarify that all consequences should be considered, but that utilities should focus efforts to "protect against" the consequences that are most concerning and relevant to their specific circumstances.

The Group discussed the transportation of hazardous materials to water utilities. There was a diversity of views on the Group as to the extent to which active and effective water utility security programs were responsible for addressing transportation of hazardous materials; however, there was agreement that transportation was an important issue and that safe transportation should be established as a clear responsibility for someone.

The Group agreed that the tentative areas of agreement on program scope should be developed into draft text on findings and recommendations for further consideration.

Program Goals, Objectives and Principles

The WSWG had a brief discussion of program goals, objectives, and principles, and agreed that the tentative areas of agreement should be developed into draft text on findings and recommendations for further review.

Program Features

The WSWG deliberated extensively on the features that make up an "active and effective" security program. Much of these deliberations were taken up with discussions of ways to categorize, organize, or group program features. The WSWG experimented with three ways to organize program features.

The Group discussed organizing program features along the dimensions of an active and effective security program. The dimensions discussed by the WSWG were personnel security, information (or cyber) security, physical security, and operational security. The Group also discussed using the program dimensions as a way to describe implementation considerations for each program feature. While this effort had some resonance, it seemed likely to create a fair amount of overlap and duplication in program feature descriptions. The Group ultimately agreed that the program dimensions are a useful way to conceptualize construction of a security program and integration of a security program into a utility operation; however, they were not satisfied with program dimensions as an overarching organizational structure for security program features. Some program dimensions (e.g., personnel security) were ultimately elevated to stand-alone security program features.

The WSWG also discussed organizing features of an active and effective security program according to steps in a continuous improvement model: plan, do, check, and adapt. There was strong convergence in the Group about the usefulness of a continuous improvement model, and the need for active and effective security programs to be managed for continuous improvement.

However, the plan, do, check, and adapt categories ultimately did not seem useful as an organizing structure for security program features, as many of the program features under discussion in the group would have planning, doing, checking, and adapting elements. For example, an up-to-date vulnerability assessment will have elements of planning, doing (assessment), checking (monitoring), and adapting, and will also have elements of human, information, physical, and operational security. After considering ways to combine organization structures based on continuous improvement elements and security program dimensions, the Group decided that the idea of continuous improvements was best addressed as a stand-alone recommendation, and that program dimensions will be addressed in the descriptive text of the WSWG report and will be incorporated into the findings and recommendations on the scope of an active and effective security program.

Finally, the WSWG discussed organizing features of an active and effective security program using the stages of emergency preparedness and response: prevention, preparedness, mitigation, response, and recovery. The Group was very comfortable with the stages of emergency preparedness and response and their relevance to an active and effective security program, and agreed that these stages should be identified and discussed in the WSWG report. However, they were ultimately not comfortable using the stages of emergency preparedness and response as an organizing structure for security program features, as many program features under discussion in the group would cut across stages of emergency preparedness and response. For example, an overarching security policy or "master plan" might address all stages of emergency preparedness and response, and therefore could not be neatly placed in one stage or another. As with program dimensions, the Group decided that the stages of emergency preparedness and response will be addressed in the descriptive text of the WSWG report and will be incorporated into the findings and recommendations on the scope of an active and effective security program. This should not be read as marginalizing the importance of the stages of emergency preparedness and response, as the Group discussed them as very important aspects of implementation of most security program features. For example, the idea of "prevention" will be an important part of program features addressing overarching security plans and policies, security spending priorities, intrusion detection and access control, and design/construction standards.

The Group ultimately decided to consider fifteen stand-alone security program features. These are not meant to be an exhaustive list of all security program features; rather, they are meant to purposefully emphasize the key features that define an active and effective security program. They are a deliberate selection of "wheels" that already exist, rather than a reinvention of the wheel. The Group discussed this as identifying the "what should you do" from the "what could you do." The Group recognized that these features need further refinement and that some features may be combined (or eliminated) in future discussions. The fifteen security program features under discussion are as follows.

1. Corporate security mission statement and security improvement plan
2. Vulnerability assessment that is up-to-date
3. Dedicated security resources and security implementation and priorities
4. Defined security roles
5. Personnel security policy, procedures, and tracking
6. Intrusion detection and access control
7. Integrated security technology policy, procedures, and tracking
8. Vital information protection
9. Contamination detection
10. Design/Construction standards

11. Threat level-based protocols
12. Emergency response and recovery plans that are up-to-date
13. Communications (internal and external)
14. Partnerships
15. Exercises

The Group anticipates that each security program feature will be described in a stand-alone recommendation, and will be written to emphasize the need for tailoring to the individual circumstances and characteristics of each utility (e.g., big v. small, urban v. rural). Text will also describe WSWG members' experience with each security program feature to emphasize key things to think about in implementation, or effective tools, guidance, or implementation approaches to consider. In addition, the Group decided to develop stand-alone recommendations on the importance of continuous improvement in an active and effective security program, and on the need to develop a security program culture throughout utility organizations.

The WSWG decided to use small groups to further refine and describe the security program features. Four small groups were considered, but one group did not garner any volunteers, so the security program features were divided among three small groups.

- Task Team C: recommendations on program features 1 – 5, 7, and 8: Doug Anderton Jeff Cooley, Jack Betkoski, Nick Catarantzos, David Siburg, and John Young.
- Task Team D: recommendations on program features 9 – 11, 6, and recommendation on security program culture: David Binning, Mike Gritzuk, Mark Miller, and Paul Orum.
- Task Team E: recommendations on program features 12 – 15, and recommendation on continuous improvement: Gregg Gruenfelder, Jennifer Nuzzo, Marc Miller, Bud Schardein, and Jasper Welsch.

Discussion of Tactical-Level Security Experiences

On October 27, 2004, during closed session, the WSWG discussed individual members' tactical-level implementation experiences with security. This discussion was organized around security program dimensions and included discussion of tactics related to personnel security, information security, physical security, and operational security. It also included discussion of members' tactical-level implementation experience related to developing partnerships with non-utility responders, interdependent infrastructure organizations, and communities.

Discussion of Incentives

On October 29, 2004, the WSWG began discussion of the second part of their mission: recommendation on mechanisms to provide recognition and incentives that facilitate a broad and receptive response among the water sector to implement an active and effective security program. The Group again discussed incentives as ways to "motivate" utility owners and operators to implement security program enhancements.

The WSWG discussed that individuals are often motivated by a sense of benefit, and discussed the benefits that utilities might realize from implementation of an active and effective security program. The Group identified the following potential benefits.

- More efficient/effective operations through inherently more productive practices.
- A more safe and secure working environment and community.

- Better understanding and support in the community, so rate payers will tolerate higher rates corresponding to safer operating conditions.
- Liability for utility owners and operations may be reduced, insurance costs may be reduced.
- Regulatory flexibility might be offered if, for example, a permit or regulatory violation is caused as a consequence of a successful attack.
- Utilities might realize better bond ratings.
- Utility performance and product might be more reliable and trusted, increasing community approval ratings and public trust.

The Group discussed that the primary motivating factors for utilities to implement security program enhancements were utility owners and operators' commitment to the public trust, and the motivation to create a safe working environment. The Group discussed that utility owners and operators are automatically motivated to implement security enhancements because of their desire to protect their customer and brand loyalty. In this context, however, the Group also discussed a number of ways that security program enhancements might be helped to compete more effectively for budget and attention against other activities (i.e., "incentives"). The Group identified the following potential incentives.

- Recognition of utility security performance by including security considerations in existing performance monitoring systems (such as the capacity rating), or by creating a report card or other recognition system.
- Explicit inclusion of security considerations in the criteria for grant and other funding.
- Explicit inclusion of security considerations in the criteria that rate setting organizations use for normal rate decisions and decisions about surcharges.
- Technical assistance, particularly for small utility operators, and better, more reliable information on security expectations and product performance.
- Ability to avoid or reduce the potential for legal wrangling, court cases, and/or findings of legal liability.
- Better insurance or bond ratings.
- Public pressure for security enhancements.
- Regulation.

The Group had a range of views about all these potential incentives, with some members more comfortable with some incentives than with others.

With respect to recognition, the Group discussed that the utility business is competitive and that owners and operators can often be motivated to improve service through peer pressure, so that knowledge of how well other utilities are doing may motivate performance.

With respect to regulation, there remains a diversity of views among the WSWG about the role that regulations might play. Some members support responsible regulations as a key incentive for security program enhancements. Other members are less comfortable with considering regulations, and instead suggest that motivation should be as strong as possible, stopping just short of regulations.

The Group also discussed, but did not resolve, how formal or independent a recognition or verification system might need to be. For example, a relatively informal, unverified system might be adequate to provide information on performance to other utilities, and in that way motivate security enhancements through peer pressure. On the other hand, financial markets might require independent verification of security enhancements before raising bond ratings or lowering insurance premiums.

The Group will continue the discussion of incentives at the December meeting.

Remarks of Michael Shapiro, EPA Deputy Assistant Administrator for Water

On October 29, 2004 Michael Shapiro addressed the WSWG. Mr. Shapiro discussed the great progress that the water sector has made in recent years to complete vulnerability assessments and develop emergency response plans. He explained that in EPA's view, the water sector is at a critical phase of moving beyond identification of risk to risk reduction—that is, moving from conducting vulnerability assessments to adopting measures that increase security and address weaknesses. Mr. Shapiro emphasized that an attack or even a credible threat of an attack on water infrastructure could have serious consequences. He thanked the Group for their service and reiterated EPA's commitment to supporting the WSWG in their deliberations.

Update on the Water Sector Coordination Council

Mr. Bennett provided an update on the Water Sector Coordination Council (Council). The Council is made up of representatives of the utility sector. Each of the eight largest trade associations for water and wastewater utilities identified one staff person and two members, and these twenty-four representatives make up the Council. Mr. Bennett is vice-chair of the council. Michael Gritzuk and Ms. Van deHei are members of the Council.

The Council held its first meeting in October. Because it is early in their process, the Council is focused on refining their operating and governance procedures and identifying discussion topics. Discussion topics identified to date include the relationship of the new DHS Homeland Information Security Network to the WaterISAC, and review of security practices recommendations that are made by the WSWG. Mr. Bennett and fellow Council members emphasized that the Council is committed to ensuring close coordination with the WSWG to avoid any duplication of effort.

The WSWG discussed a number of differences between themselves and the Council. These include group membership (the WSWG is made up of utility representatives and other stakeholders—the Council is limited to utility representatives), timing (the WSWG will end after five meetings—the Council does not have a specified end date), and mission (the WSWG was given a specific mission from the NDWAC—the Council will create its own agenda). The Group agreed that close coordination with the Council is important.

WSWG Draft Operating Procedures

The WSWG discussed their revised draft operating procedures on October 27, 2004. Revisions to the draft operating procedures were made to address comments made during the first in-person WSWG meeting and include adding procedures for identifying and addressing security-sensitive information, clarifying the role of staff to WSWG members, and clarifying the distribution procedures for draft documents. Rob Greenwood, of Ross & Associates, briefly reviewed the revised draft WSWG operating procedures.

With respect to identification of security-sensitive information, the WSWG again ratified the definition of security sensitive information they discussed at their first in-person meeting:

- 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.

Within this definition, the Group agreed that 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. The Group agreed that there should be a "low threshold" for identification of security-sensitive information. If one member asserts that information is security sensitive, the group will respect that assertion and manage the information in accordance with the operating procedures for security-sensitive information.

With respect to managing security-sensitive information, the WSWG ratified the provisions, including the security pact, in the revised draft operating procedures. One WSWG member asked what the incentive was for members to conform to the confidentiality pact and manage security-sensitive information appropriately. The WSWG discussed their mutual commitment to one another and to safeguarding the nation's water infrastructure and resources, and the use of peer pressure, as factors that would encourage adherence with the security pact. The Group also discussed the application of federal laws governing information security for certain types of information that may be covered under the Bioterrorism Act. (Although it is unlikely that this would apply in that the Group as a whole does not hold a security clearance and it is not planned that they would receive any information that is legally restricted.) The WSWG affirmed that to maximize the usability of their products, they will strive to limit the inclusion of security-sensitive information in written materials coming to and produced by the Group.

The WSWG discussed the role of staff of WSWG members and the distribution of draft documents. The Group affirmed that it is not appropriate for staff of WSWG members to independently comment on draft documents, and that the comments on draft documents should be submitted by WSWG members.

The Group discussed reporting to the NDWAC and clarified that, for purposes of the upcoming November NDWAC meeting, the three WSWG members who also serve on the NDWAC will provide an update on Group activities. Finally, the Group discussed the mission statement and confirmed that they interpret the first part of the mission to include source waters, and that they are approaching the mission to identify "best security practices" by defining and describing the characteristics of an "active and effective" security program.

Discussion of Future WSWG Meetings

The WSWG discussed the status of their deliberations to date. Two meetings are complete and three additional meetings are planned. Work has focused on describing an active and effective security program; however, the Group must quickly stabilize security discussions so the focus can shift to the other two aspects of the WSWG mission: (1) mechanisms to provide recognition and incentives that facilitate a broad and receptive response among the water sector to implement active and effective security programs; and (2) mechanisms to measure the extent of implementation of active and effective security programs. Many WSWG members see identification of measures of the effectiveness of security programs as the most difficult aspect of the Group's mission.

In light of this challenge, the Group agreed that at future meetings presentations should be strictly reviewed for relevancy to the WSWG mission and deliberations, and that outside presentations should be minimized in favor of deliberations, including (if needed) presentations by WSWG members. This was discussed as "no more nice to know." The Group identified a

number of specific potential topics for future meetings, as follows.

- Information on community involvement and how to effectively reach out to communities to increase responsiveness and trust.
- Information on how best to instill cultural change in an organization, for purposes of exploring how best to promote a security culture in water utilities.
- Information about EPA's work to create verification systems around measures.
- Information about existing approaches to measuring the effectiveness of preventative programs, the measures required in the National Infrastructure Protection Plan, and general measures of effectiveness in EPA water programs.
- Information on key attributes of successful response and recovery planning, and coordination from non-utility first responders and/or exercise evaluators.
- Information on potential sources of funding for security enhancements, including grant and other funding from DHS.

Presentations to the WSWG

The WSWG considered six presentations during the October meeting. On October 27, 2004, Irv Pikus from the American Society of Civil Engineers gave a presentation on efforts to develop guidance on physical security tactics, including real-time contaminant monitoring techniques. Also on October 27, 2004, John Porco from Michael Baker Corporation gave a presentation on development and key features of the Security Practices Primer for Water Utilities.

On October 28, 2004, Lew Leffler from the North American Energy Reliability Council gave a presentation on the electric utility sector's work to develop an industry security standard and guidelines. Also on October 28, 2004, Dorothy Kellogg from the American Chemistry Council and Jack Aherne from the Chlorine Institute gave presentations on, respectively, the security-related aspects of the Responsible Care program for chemical manufacturers and voluntary security guidelines for chlorine manufacturers and distributors.

On October 29, 2004, Rob Greenwood from Ross & Associates gave a presentation summarizing ongoing research on incentives for adoption of security enhancements.

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 D – I.

Public Comment

No individuals offered comment at the WSWG meeting and no written comments were received.

Meeting Wrap-Up and Next Steps

Mr. Binning closed the WSWG meeting by observing that, although deliberations had at times been difficult, good progress towards describing an active and effective security program was made, and by thanking WSWG members for their attention and participation.

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

- WSWG members will review the draft EPA and DHS document on Agency roles and responsibilities and forward any questions to Marc Santora (santora.marc@epa.gov). EPA and DHS will continue to refine and finalize the document.
- Ross & Associates will make final revisions to the WSWG operating procedures and provide a final draft revised procedures to the WSWG to review.
- Ross & Associates will draft text on WSWG security program deliberations, and the scope, goals, objectives, and principles of an active and effective security program for WSWG review.
- Ross & Associates will organize meetings of three WSWG task teams to further define and describe features of an active and effective security program, and will provide materials to task teams for review.

In accordance with the WSWG project plan, the December meeting of the WSWG will be focused around: (1) stabilizing draft recommendations on active and effective security programs, and (2) framing draft recommendations on incentives. Opportunities for the WSWG to go into closed session will be provided for use, if needed.

Attachments

Meeting Materials—Non-Draft Documents

Attachment A: Meeting Agenda
Attachment B: NDWAC Working Group Ground Rules
Attachment C: WSWG Project Plan
Attachment D: Presentation of Irv Pikus, dated October 27, 2004
Attachment E: Presentation of John Porco, dated October 27, 2004
Attachment F: Presentation of Lew Leffler, dated October 2004
Attachment G: Presentation of Dorothy Kellogg, dated October 2004
Attachment H: Presentation of Jack Aherne, dated October 2004
Attachment I: Presentation of Rob Greenwood, dated October 29, 2004

Meeting Attendance and Participation

Attachment J: WSWG Roster and Contact List
Attachment K: List of Others in Attendance

Additional Meeting Materials—Draft Documents, Not Attached

- WSWG Revised Draft Operating Procedures, dated October 19, 2004
- EPA and DHS Roles and Responsibilities, dated October 27-29, 2004
- Draft annotated bibliography of security-related resources, dated October 22, 2004