Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex

ISBN
978-0-309-20884-0

30 pages
8 1/2 x 11
PAPERBACK (2011)

Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex; National Research Council

UNDERSTANDING AND MANAGING RISK IN SECURITY SYSTEMS FOR THE DOE NUCLEAR WEAPONS COMPLEX

(Abbreviated Version)

Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex

Nuclear and Radiation Studies Board
Division on Earth and Life Studies

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Award No. DE-DT0000109, TO#27 between the National Academy of Sciences and the U.S. Department of Energy, National Nuclear Security Administration, Office of the Associate Administrator for Defense Nuclear Security. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-20884-0
International Standard Book Number-10: 0-309-20884-X

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu

Printed in the United States of America

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON RISK-BASED APPROACHES FOR SECURING THE DOE NUCLEAR WEAPONS COMPLEX

CHRIS G. WHIPPLE (*Chair*), ENVIRON International Corporation, Emeryville, California
GEORGE APOSTOLAKIS, Massachusetts Institute of Technology, Cambridge, Massachusetts[1]
W. EARL BOEBERT, Sandia National Laboratories (retired), Albuquerque, New Mexico
D. JEFFREY BOSTOCK, Lockheed Martin Energy Systems (retired), Seabrook Island, South Carolina
ROBIN L. DILLON-MERRILL, Georgetown University, Washington, D.C.
ROGER L. HAGENGRUBER, University of New Mexico, Albuquerque
JOSEPH KROFCHECK, Independent Consultant, Warrenton, Virginia
WILLIAM L. MCGILL, The Pennsylvania State University, University Park
THOMAS MOSER, Applied Research Associates, Inc., Wilmington, North Carolina
DAVID J. OSIAS, Centra Technologies, Inc., Arlington, Virginia
DANIEL M. SCHUTZER, Financial Services Technology Consortium, Boca Raton, Florida
BRIAN SNOW, National Security Agency (retired), Clarksville, Maryland
FRANCIS TAYLOR, General Electric Company, Fairfield, Connecticut
MARY D ZALESNY, Pacific Northwest National Laboratory, Seattle, Washington

Staff

SARAH C. CASE, Study Director
KEVIN D. CROWLEY, Director, Nuclear and Radiation Studies Board
MICAH D. LOWENTHAL, Director, Nuclear Security and Nuclear Facility Safety Program
TONI GREENLEAF, Administrative and Financial Associate
ERIN WINGO, Senior Program Assistant
JAMES YATES, JR., Office Assistant

[1] Resigned March 26, 2010.

NUCLEAR AND RADIATION STUDIES BOARD

Preface to the Abbreviated Version

This is an abbreviated version of the National Academies' report on augmenting DOE's security systems at sites in the nuclear weapons complex, and particularly on the applicability of risk assessment concepts for this augmentation. The full report is entitled *Understanding and Managing Risk in the DOE Nuclear Weapons Complex.* The full version of that report, which is exempt from public release under the Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(2), was issued in November 2010.

Chris Whipple, Chair

Preface

This study was requested by the Senate Appropriations Committee in response to what that committee saw as unsustainable rates of increase in the cost of security at the U.S. Department of Energy (DOE). In current-year dollars, security costs have increased from $550 million in 2002 to around $930 million in 2010. For decades, DOE has been setting its security requirements based on a design basis threat (DBT). Under such an approach, DOE headquarters specifies characteristics of an attacking force, and, using field exercises and combat simulation software, its facilities determine the defensive resources needed to successfully repel the threat. Over the past decade, this approach has led to the significant cost increases noted above. The DBT is now being replaced with an approach called the Graded Security Protection Policy.

The specific question that the authoring committee of this report (the study committee) was asked to address is whether risk-based approaches, including probabilistic risk assessment, could be used to improve DOE's methods for determining its security posture and requirements. As described in this report, the study committee judges that the conceptual approaches used in risk assessments for contexts other than security can provide a helpful framework for DOE security. However, the committee could not identify how to assess the types of attacks that might occur and their associated probabilities, something necessary for a fully quantitative approach.

DOE has been working over the past decade to effectively reduce risk. However, the committee has several suggestions that could improve the way that DOE considers risk. In particular, one aspect of DOE's approach over the past decade has been to consolidate special nuclear material (SNM) into fewer facilities that are more easily defended than current facilities. Significant progress has been made in "shrinking the footprint," as this approach is described. DOE has succeeded in removing all remaining weapons-usable material from the Hanford site and has announced a plan to do the same at Lawrence Livermore National Laboratory within a few years. In addition, the National Nuclear Security Administration (NNSA) in DOE added robust physical barriers to protect sensitive materials by constructing a new facility at the Y-12 National Security Complex and by upgrading the security features of the K-Reactor facility at the Savannah River Site. Security of materials being transported also remains a concern.

The committee was charged with addressing how risk-based approaches to security management could augment security and help managers to find an appropriate balance between physical security and cyber security. Our focus regarding cyber security was with interactions between computer systems and physical security. We did not address the potential for loss of sensitive information or documents through compromised computer systems.

It is the committee's view that the various security elements need to be addressed in an integrated way. The committee judges that the current approach underinvests in some areas and that better integration is needed to plan for some types of attacks on nuclear weapons or SNM.

Chris G. Whipple, *Chair*

Acknowledgments

Over the course of this study, the committee added a great deal to its knowledge about the physical, cyber, and personnel security systems that DOE and other agencies have in place to protect nuclear weapons and material. The committee received many briefings and was permitted to view the security systems in place at a number of facilities. Its questions were nearly always answered with clarity and candor. This report could not have been written without the support of the people listed below who made presentations to the committee and/or met with small groups of committee members. The information and cooperation that the committee received from these organizations and individuals were critical to the success of this study.

The committee would particularly like to acknowledge the excellent support it received from the project sponsor, the U.S. Department of Energy, National Nuclear Security Administration. The committee is especially grateful for the support it received from Bradley Peterson, Douglas Fremont, Kevin Leifheit, and Michael Collier.

The committee gratefully acknowledges the following people who made presentations at its information-gathering sessions:

- Gregory Baum, Betty Biringer, Derek Farr, Brady Pompei, Brian Rigdon, J. R. Russell, Joe Sandoval, Mike Skroch, Frederick Sexton, Andrew Walter, and Gregory Wyss, Sandia National Laboratories;
- Devin Biniaz and Col. Patrick Vetter, Office of the Deputy Assistant to the Secretary of Defense (Nuclear Matters), U.S. Department of Defense;
- Penney Harwell Caramia, Jonathan Gill, and Bob Repasky, U.S. Government Accountability Office;
- Edith Chalk and Thomas Callander, U.S. Department of Energy (DOE), Office of Classification;
- E. Bruce Held, Sandia Senior Counterintelligence Officer (formerly);
- David Higgins, DOE Office of Intelligence and Counterintelligence;
- Mark Jackson, Rob Aaron, and Jim Blankenship, DOE Office of Secure Transportation;
- Ever Morales, U.S. Defense Intelligence Agency;
- Glenn Podonsky and Sam Callahan, DOE Office of Health, Safety and Security;
- Bradley Peterson and Kevin Leifheit, U.S. Department of Energy, National Nuclear Security Administration, Defense Nuclear Security;
- Special Agent David Raymond, Federal Bureau of Investigation, Albuquerque Field Office;
- Paul Sowa, B&W Technical Services;
- Mike Stockdale, Nick Pera, and Robert Appleton, Strategic Systems Program, U.S. Department of the Navy;
- Peter Stockton, Project on Government Oversight;
- Roberta Warren and Barry Westreich, U.S. Nuclear Regulatory Commission; and
- Linda Wilbanks and Wayne Jones**,** U.S. Department of Energy, National Nuclear Security Administration Office of the Chief Information Officer.

The committee visited a number of sites during this study to obtain first-hand information about the security measures in place at facilities that secure nuclear weapons and materials. We gratefully acknowledge the following organizations and individuals for supporting these visits and providing briefings about the security measures in place:

- Los Alamos National Laboratory and Site Office: Harold Brocklesby, Mike Lansing, Jack Killeen, Kirk Ellard, Ken Freeman, Tom Harper, Valorie Livesay, Kim Nelson, and David Telles
- Sandia National Laboratories and Site Office: Ronald Moya, M. Bradley Parks, Anthony Aragon, and Eileen Johnston
- Y-12 National Security Complex and Site Office: Ted Sherry, Darrel Kohlhorst, Dexter Beard, Richard Glass, John Howanitz, J. Travis Howerton, Bill Klemm, and Tom Smith
- Pantex Plant and Site Office: Steve Erhart, Jack Killeen, Tyfani Lanier, Clay Messer, Reuben McGilvary, Kristy McWilliams, Jeremy Scott, Larry Spaulding, and Roxanne Steward
- Savannah River Site and Site Office: Chris Amos, Robert Edwards, Kevin Hall, Roxanne Jump, Jim Tomack, Bob Weatherby, and Thomas Williams
- Kirtland Air Force Base: Lt. Col. Eric Y. Moore, Capt. Nathan M. Murray, and MSgt. Eric S. Smith
- Kings Bay Naval Base: Capt. M. (Rusty) Nagle, Lt. Col. Whiteside, and Cdr. Allan Andrews.

We also thank Lee McLemore at Lawrence Livermore National Laboratory for his graciousness in arranging for space in which the committee chair and staff were able to meet to discuss the progress of the report and work on drafts. In addition, the regular assistance of several authorized derivative classifiers at DOE—Irwin Binder, Vincent Vecera, and Julia Schucker—was invaluable in producing this study in a timely and secure fashion.

The committee is also grateful for the excellent assistance provided by the National Research Council staff in preparing this report. Staff members who contributed to this effort are Sarah Case (study director), Micah Lowenthal (director of the Nuclear Security and Safety Program), Kevin Crowley (director of the Nuclear and Radiation Studies Board), Erin Wingo (senior program assistant), and Toni Greenleaf (financial and program associate).

Finally, I thank the committee members for their dedicated work throughout the development of this report, including George Apostolakis, who resigned from the committee when he was appointed to the U.S. Nuclear Regulatory Commission.

Chris G. Whipple, *Chair*

Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the Report Review Committee of the National Research Council (NRC). The purpose of this independent review is to provide candid and critical comments that will assist the NRC in making its published report as sound as possible and will ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We thank the following individuals for their participation in the review of this report:

- Dr. Jay Davis, Hertz Foundation;
- Dr. Barry Ezell, Old Dominion University;
- Dr. Robert A. Frosch, John F. Kennedy School of Government, Harvard University;
- Dr. B. John Garrick, Independent Consultant;
- Dr. Michael Gelles, Deloitte Consulting;
- Gen. John A. Gordon, U.S. Air Force (retired);
- Mr. John Keesling, National Reconnaissance Organization;
- Mr. Bob McCants, Lockheed Martin Corporation;
- Adm. Richard Mies, Independent Consultant;
- Mr. Rolf Mowatt-Larssen, John F. Kennedy School of Government, Harvard University;
- Dr. Randall Murch, Virginia Polytechnic Institute and State University; and
- Mr. John Stenbit, Department of Defense and TRW, Inc. (retired).

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by John Ahearne, Executive Director Emeritus of Sigma Xi, and Cherry Murray, Dean of the Harvard School of Engineering and Applied Sciences. Appointed by the National Research Council, they were responsible for making certain that an independent examination of the report was carried out in accordance with institutional procedures and that all review comments were considered carefully. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Contents

Executive Summary

A nuclear weapon or a significant quantity of special nuclear material (SNM) would be of great value to a terrorist or other adversary. It might have particular value if acquired from a U.S. facility—in addition to acquiring a highly destructive tool, the adversary would demonstrate an inability of the United States to protect its nuclear assets. The United States expends considerable resources toward maintaining effective security at facilities that house its nuclear assets. However, particularly in a budget-constrained environment, it is essential that these assets are also secured efficiently, meaning at reasonable cost and imposing minimal burdens on the primary missions of the organizations that operate U.S. nuclear facilities.

It is in this context that the U.S. Congress directed the National Nuclear Security Administration (NNSA)—a semi-autonomous agency in the U.S. Department of Energy (DOE) responsible for securing nuclear weapons and significant quantities of SNM—to ask the National Academies for advice on augmenting its security approach, particularly on the applicability of quantitative and other risk-based approaches for securing its facilities. In carrying out its charge, the committee has focused on what actions NNSA could take to make its security approach more effective and efficient.

The committee concluded that the solution to balancing cost, security, and operations at facilities in the nuclear weapons complex is not to assess security risks more quantitatively or more precisely. This is primarily because there is no comprehensive analytical basis for defining the attack strategies that a malicious, creative, and deliberate adversary might employ or the probabilities associated with them. However, using structured thinking processes and techniques to characterize security risk could improve NNSA's understanding of security vulnerabilities and guide more effective resource allocation.

Over the course of the study, the committee identified three key shortcomings in NNSA's current security approach: (1) the interactions and dependencies among security countermeasures;[2] (2) the interactions between DOE/NNSA and other organizations responsible in part for preparing for or responding to an attack on NNSA facilities; and (3) the adequacy of attack scenarios used to design, update, and test the security systems to consider all possible attack scenarios.

As a first step in addressing these shortcomings, the committee recommends that NNSA adopt what the committee termed a "total systems approach" to characterize the interactions and dependencies of security countermeasures at its facilities. Such an approach is commonly used as an initial step in assessing the risks associated with a complex technological system. However, performing such an analysis is not sufficient for implementing highly effective security. Coordination, communication, and joint exercises that include all relevant security organizations are also necessary.

In addition, it is essential to understand the adversary. This involves understanding adversary objectives, goals, and, in particular, how adversaries view the security system. The committee's approach could help DOE to better understand a range of potentially unexpected vulnerabilities and attack scenarios.

Historically, DOE has emphasized some security countermeasures over others in protecting nuclear weapons and SNM, potentially leading to opportunity costs and hidden

[2] The committee restricted its focus to cyber security directly associated with the physical protection of nuclear weapons and materials. The project sponsor agreed to this interpretation in September 2009.

vulnerabilities. A total systems approach could better integrate these security elements and account for their inherent interdependencies. A total systems approach incorporating all security countermeasures could also lead to better prioritization of which security risks and vulnerabilities will be mitigated.

Summary

In the U.S. Department of Energy (DOE), the National Nuclear Security Administration (NNSA)—a semi-autonomous agency—is responsible for securing fully and partially assembled nuclear weapons and significant quantities of special nuclear material (SNM). NNSA's security mission includes protecting these weapons and materials, associated facilities, and other assets.

In the current budget-constrained environment, NNSA's security system needs to be both effective and efficient. An effective NNSA security system would be robust, resilient, and adaptive. An efficient NNSA security system would operate at reasonable cost and impose minimal burdens on the organizations carrying out NNSA's primary missions at its facilities.

Previous examinations of NNSA's security (Mies 2005; GAO 2007a, b, 2010) have found that security at NNSA sites has been neither resilient nor adaptive. In addition, as a result of DOE's[3] security expansion in the wake of the attacks of September 11, 2001, until recently costs were escalating at unsustainable rates. At the same time, the increased security requirements have made many of the sites' primary mission activities much more burdensome. DOE and NNSA recently issued a revised security policy, the Graded Security Protection (GSP) Policy, intended to address some of these concerns.

It is in this context that the U.S. Congress directed NNSA to ask the National Academies for advice on augmenting its security approach, particularly on the applicability of probabilistic risk assessment and other risk-based approaches to securing the complex. In carrying out its charge (see Appendix A), the committee has focused primarily on what actions DOE and NNSA could take to make their security approach more effective and efficient.

The committee has concluded that defining security risks more precisely (e.g., by using a probabilistic risk assessment approach) will not significantly improve NNSA's security planning. This is primarily because there is no comprehensive analytical basis for defining the attack strategies an adversary might employ or the probabilities of success associated with them.

However, this does not mean that a rigorous assessment of security risk is not useful. Using structured thinking processes and techniques to characterize security risk could improve NNSA's understanding of security vulnerabilities. In addition, understanding the risks and uncertainties associated with various security subsystems as well as the security system as a whole can inform and improve decisions, particularly in allocating limited resources, provided the techniques are used appropriately.

Still, there is no single comprehensive approach that can ensure an effective and efficient security system. In particular, risk methodologies cannot address cultural or organizational barriers to improved security, and no risk approach can determine how much DOE's nuclear security program should cost. Decisions about how much risk can and should be accepted are the responsibility of the U.S. government and inherently rely on nontechnical considerations.

With these considerations in mind, in this report, the committee focuses on how NNSA could use risk-based analysis and other approaches to better inform decision making, particularly related to the following three key shortcomings associated with NNSA's current nuclear security system that were identified by the committee:

1. The interactions and dependencies among security countermeasures;

[3] The "nuclear weapons complex" encompasses facilities operated by NNSA. However, other organizations within DOE operate facilities that manage and protect Category I SNM, including the DOE Office of Science and the DOE Office of Environmental Management. DOE-wide policies apply to all facilities; other policies and procedures are NNSA specific. In this report, DOE is referred to when policies applying to all DOE facilities are discussed; NNSA is referenced when policies and procedures specific to the nuclear weapons complex are discussed.

2. The interactions between DOE/NNSA and other organizations responsible in part for preparing for or responding to an attack on NNSA facilities; and
3. The attack scenarios used to design, update, and test the security systems.

The committee judges that its recommendations regarding these shortcomings—in particular, that DOE adopt a "total systems approach" to security, described in detail in Chapters 3 and 4 of the full report—can help DOE better evaluate facility security systems and their vulnerabilities. However, the committee has refrained from outlining a specific methodology; it instead focused on general approaches and tools that could be used.

The committee's major recommendations are described below and are discussed in detail in the body of the full version of the report.

A dissenting opinion from one committee member is included in the full version of the report. This opinion is largely consistent with the report's findings and recommendations, but it emphasizes a need for a single entity with both the responsibility and authority to direct the security system.

Finally, the committee limits its scope to cyber security as it relates to the physical security of nuclear weapons and significant quantities of SNM. Neither this report nor the full report addresses the cyber security aspects of protecting classified information or documents. This interpretation of the committee's scope was agreed on with the sponsor in September 2009.

KEY RECOMMENDATIONS

In this section, the committee describes and briefly explains the key recommendations contained in the committee's report. The committee's work also resulted in a number of findings, that were judged to be too sensitive to reproduce in this abbreviated version. The findings are included in the full version of the report, entitled *Understanding and Managing Risk in the DOE Nuclear Weapons Complex*, which is exempt from public release under the Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(2).

RECOMMENDATION 3-1: The committee advises against the use of probabilistic risk assessment (PRA) in designing security for the DOE nuclear weapons complex at this time. However, the committee recommends the use of some tools and techniques traditionally associated with PRA to improve NNSA's understanding of the full spectrum of risks to the complex.

RECOMMENDATION 3-2: NNSA should utilize relevant techniques traditionally associated with risk assessment to improve its understanding of risk—specifically including an analysis of the security system—along with creative scenario generation techniques and security best practices.

RECOMMENDATION 4-1: The committee recommends that DOE/NNSA generate a range of plausible and specific objectives that the site security system is intended to preclude, for use in scenario generation. An adversary perspective should be taken into account when generating these objectives.

RECOMMENDATION 4-2: The committee recommends that a comprehensive and plausible range of adversary capabilities, strategies, and tactics be considered in defining the threat to sites and designing security systems.

RECOMMENDATION 4-3: The committee recommends that DOE sites regularly track and evaluate the information available to an adversary and use this information to improve their understanding of the most likely ways an adversary might attack a given site or other operations, such as transportation.

RECOMMENDATION 4-4: The committee recommends that DOE sites supplement their current vulnerability assessment processes with creative scenario generation techniques.

RECOMMENDATION 4-5: The committee recommends that DOE Headquarters take on the responsibility of defining an overall deterrence strategy for the nuclear weapons complex, subject to evaluation by deterrence subject-matter experts.

RECOMMENDATION 5-1: The committee recommends that DOE focus its communication efforts aimed at Congress and the administration on risk management rather than on the risk to the nuclear weapons complex. This communication should draw on the total systems approach and scenario generation processes recommended by the committee.

RECOMMENDATION 5-2: The committee recommends that DOE take steps to ensure a more integrated and collaborative environment for functional responsibility for the security system at the headquarters level and in the field. A clearer and more expeditious process for accepting risk should be a priority goal.

CONCLUSION

It is clear that the threat that DOE requires its sites to defend against is formidable. The current security emphasis is out of balance. A redirection of focus and resources is indicated, but accomplishing such a major shift in approach will require leadership and a different model for security guidance, planning, and evaluation. The committee's recommendations are intended to serve as a starting point for this change.

Of the recommendations listed above, three stand out in the committee's view as its primary suggestions for how DOE/NNSA could effectively succeed in restructuring its security approach. These suggestions are primarily related to the lack of a total systems view associated with security at NNSA sites.

First, DOE/NNSA should seek to better integrate its security efforts. This would help to address potentially significant vulnerabilities. Second, NNSA and other outside security organizations that are responsible for some aspects of the security of the weapons complex do not appear to be well coordinated. Third, a broader suite of adversary scenarios should be developed.

Finally, the committee notes that any analysis is only an input to a decision maker who needs to make a subjective judgment regarding defense strategies, tactics, and investments. Despite the best plans, defenses, and training, the decision maker needs to be alert and prepared to react quickly and decisively to the unexpected. Thus, it is essential that all aspects of security associated with the DOE nuclear weapons complex —whether they are operated by DOE, by NNSA, or by another agency entirely—be well understood, well organized, well exercised, and well coordinated. Although this may not require changes in how NNSA's security apparatus is organized, it is likely to require a change in approach and a change in mindset.

References

Mies, R. W. 2005. NNSA Security: An Independent Review. Prepared for the National Nuclear Security Administration. Washington, DC.

U.S. Government Accountability Office. 2007a. Security and Management Improvements Can Enhance Implementation of the NNSA Act. GAO-07-428T. Washington, DC: U.S. Government Accountability Office.

U.S. Government Accountability Office. 2007b. Additional Actions Needed to Improve Management of the Nation's Nuclear Program. GAO-07-36. Washington, DC: U.S. Government Accountability Office.

U.S. Government Accountability Office. 2010. DOE Needs to Fully Address Issues Affecting Protective Forces' Personnel Systems. GAO-10-485T. Washington, DC: U.S. Government Accountability Office.

Biographical Sketches of Committee Members

CHRIS G. WHIPPLE (NAE), *Chair*, is a principal in the Emeryville, California office of ENVIRON International Corporation, an environmental consulting firm. His professional interests are in risk assessment, and he has consulted widely in this field for private clients and government agencies. Much of his work involves radioactive materials or mercury. Dr. Whipple is a member of the National Academy of Engineering, and currently serves as co-chair of the Academies' Report Review Committee. He previously served as chair of the National Research Council (NRC) Board on Radioactive Waste Management and as a member of the Board on Environmental Studies and Toxicology. He has served on and chaired numerous NRC committees, most recently for the NRC Committee on Medical Isotope Production Without Highly Enriched Uranium, which he chaired. He is a long-time member of the National Council on Radiation Protection and Measurements. Dr. Whipple received his B.S. in engineering science from Purdue University and his M.S. and Ph.D. in engineering science from the California Institute of Technology.

GEORGE E. APOSTOLAKIS[4] was sworn in as a Commissioner of the U.S. Nuclear Regulatory Commission (NRC) on April 23, 2010. Prior to his appointment, he was the Korea Electric Power Company Professor of Nuclear Science and Engineering and Professor of Engineering Systems at the Massachusetts Institute of Technology. His research includes developing methods for probabilistic risk assessment of complex technological systems, risk management involving several stakeholder groups, decision analysis, human reliability models, organizational factors and safety culture, infrastructure security, and risk-informed and performance-based regulation. Dr. Apostolakis has received several awards and honors, including the Tommy Thompson Award for Nuclear Safety from the Nuclear Installations Safety Division of the American Nuclear Society in 1999. Dr. Apostolakis is editor-in-chief of *Reliability Engineering and System Safety, An International Journal,* Elsevier Science Publishers, England; founder and secretary, International Association for Probabilistic Safety Assessment and Management; member and former chairman, Advisory Committee on Reactor Safeguards, U.S. Nuclear Regulatory Commission; and a member of the National Academy of Engineering. Dr. Apostolakis received his Ph.D. and M.S. in Engineering Science from the California Institute of Technology, and a Diploma in Electrical Engineering from the National Technical University of Athens.

W. EARL BOEBERT is an expert on information security, with experience in national security and intelligence as well as commercial applications. He recently retired as senior scientist at Sandia National Laboratories and currently consults for Sandia's Office of Intelligence and Counterintelligence. He has 30 years' experience in communications and computer security and is the holder or co-holder of 13 patents. Prior to joining Sandia, he was the technical founder and chief scientist of Secure Computing Corporation, where he developed the Sidewinder security server, a system that currently protects several thousand sites. Before that, he worked 22 years at Honeywell, rising to the position of senior research fellow. At Honeywell, Mr. Boebert worked on secure systems, cryptographic devices, flight software, and a variety of real-time simulation and control systems, and he won Honeywell's highest award for technical achievement for his part in developing a very large scale radar landmass simulator. He also developed and presented a course on systems engineering and project management that was eventually

[4] Dr. Apostolakis resigned from the committee on March 26, 2010.

given to over 3,000 students in 13 countries. He served on the National Research Council committees that produced *Computers at Risk: Computing in the Information Age*; *For the Record: Protecting Electronic Health Information*; and *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities.*

D. JEFFREY BOSTOCK retired from Lockheed Martin Energy Systems, Inc., as vice president for engineering and construction with responsibility for all engineering activities within the Oak Ridge nuclear complex. He has extensive experience managing projects as a U.S. Department of Energy contractor. He has also served as vice president of defense and manufacturing and manager of the Oak Ridge Y-12 plant, a nuclear weapons fabrication and manufacturing facility. His career at Y-12 included engineering and managerial positions in all of the various manufacturing, assembly, security, and program management organizations. He also served as manager of the Paducah Gaseous Diffusion Plant. He was a member of the committees that produced the National Research Council (NRC) reports *Proliferation Concerns: Assessing U.S. Efforts to Help Contain Nuclear and Other Dangerous Materials and Technologies in the Former Soviet Union* and *Protecting Nuclear Weapons Material in Russia*. Mr. Bostock has also served as a panel member for the annual NRC assessment of the National Institute of Standards and Technology Measurement and Standards Laboratories. He was also a member of the NRC Committee on Oversight and Assessment of Department of Energy Project Management, and most recently, the NRC Committee on Medical Isotope Production Without Highly Enriched Uranium. Mr. Bostock received a B.S. in industrial engineering from Pennsylvania State University and an M.S. in industrial management from the University of Tennessee. He is a graduate of the Pittsburgh Management Program for Executives.

ROBIN L. DILLON-MERRILL is an associate professor at the McDonough School of Business at Georgetown University. Her research specializes in risk and decision analysis. In particular, Dr. Dillon-Merrill's research examines critical decisions that people have made following near-miss events in situations with severe outcomes, such as hurricane evacuation, and National Aeronautics and Space Administration (NASA) mission management. She also uses programmatic risk analysis to improve project and operational management in complex, resource-constrained environments. Her past research in risk has included supporting the U.S. Department of Energy (DOE) selection of a new tritium supply facility and aiding NASA's Jet Propulsion Laboratory in decision making for past Mars missions. She is currently serving on the National Research Council (NRC) Committee on New Orleans Regional Hurricane Protection Projects, and has previously served on the NRC Committee on Assessing the Results of External Independent Reviews for U.S. Department of Energy Projects as well as the Committee on Opportunities for Accelerating Characterization and Treatment of Waste at DOE Nuclear Weapons Sites. Dr. Dillon-Merrill received her Ph.D. in engineering risk analysis from Stanford University, and an M.S. and B.S. from the University of Virginia.

ROGER L. HAGENGRUBER is the director of the Office for Policy, Security and Technology (OPS&T) and the Institute for Public Policy (IPP) and a research professor (political science and physics) at the University of New Mexico. He was formerly a senior vice president at Sandia National Laboratories and directed Sandia’s primary mission in nuclear weapons during the transition following the end of the Cold War. He spent much of his 30-year career at Sandia in arms control and nonproliferation activities including several tours in Geneva as a negotiator. In recent years, he has focused on the nuclear transition in the former Soviet Union and on security issues associated with counterterrorism and has chaired or served on numerous panels that have addressed these issues. His work at the University of New Mexico includes directing the IPP work in public surveys including sampling of U.S. and European views on a wide range of security issues. The OPS&T creates multidisciplinary teams from laboratories and

universities to explore policy options for issues in which security and technology are interrelated. He previously served on the Nuclear and Radiological Panel of the National Research Council's Committee on Science and Technology for Countering Terrorism. He received his Ph.D. in experimental nuclear physics from the University of Wisconsin and is a graduate of the Industrial College of the Armed Forces.

JOSEPH KROFCHECK is a consultant with the U.S. Department of Energy (DOE) Office of Intelligence and Counterintelligence dealing with matters of trust betrayal and related issues. He is active in the intelligence community with particular interest in the "insider problem." Before beginning his current contract with DOE (in 1984), he worked with the RAND Corporation for 11 years as a resident consultant. At RAND, he developed methodology for and ran the team that assessed communicated nuclear threats for DOE and the FBI; participated as a member of the Nuclear Emergency Search Team; participated in the development of the first design basis threat for DOE nuclear facilities and programs (a project for Sandia Labs); and worked on counterterrorism projects for DOE. He also participated in the development of the Emergency Response Plan for Nuclear Threat or Blackmail for the state of California. From 1979 to 2010, he served as the Psychiatric Consultant to the National Reconnaissance Office/Office of Security and Counterintelligence, and worked for 22 years (1972–1994) as a Specialist Reserve Officer for the Los Angeles Police Department. Dr. Krofcheck received his M.D. from the University of Southern California, and completed an internship and Psychiatric Residency at the Los Angeles County General Hospital. He received a Masters in Public Health (M.P.H.) from the University of California at Los Angeles in 1964 while on a fellowship in social and community psychiatry.

WILLIAM L. MCGILL is an assistant professor of Security Risk Analysis at the Pennsylvania State University. His research focuses on risk analysis, uncertainty modeling and decision analysis applied to homeland security, defense, and intelligence problems. His particular interests are in adversary reasoning, extreme events modeling, deception, and counterdeception. His past research focused on risk, uncertainty, and reliability analysis, including both probabilistic and nonprobabilistic methods with applications to critical infrastructure protection and the New Orleans Hurricane Protection System. Previously, as an intelligence officer with the Defense Intelligence Agency, he helped develop training courses and new methodologies for risk analysis, uncertainty modeling, and logical reasoning. In 2003–2004, Dr. McGill was the first American Society of Mechanical Engineers fellow to the Department of Homeland Security where he helped develop strategic risk analysis methodologies for infrastructure protection. Dr. McGill holds a Ph.D. in reliability engineering from the University of Maryland, is a registered professional engineer, and is a certified reliability engineer with the American Society of Quality.

THOMAS G. MOSER is a member of the Chairman's Group of Applied Research Associates Inc., where he provides antiterrorism and security expertise to federal, state, and local government and private-sector clients. Mr. Moser previously served as commanding officer of the Navy's unique RED CELL team, commanding officer of the Naval Special Warfare Development Group (a classified special SEAL unit), and as chief of staff at the Joint Special Operations Command. Following his naval career, Mr. Moser served as a counterterrorism and special operations consultant and exercise planner for Department of Defense Special Operations Units. He developed plans to exercise the nation's response to incidents involving the use of chemical, biological, radiological, and nuclear weapons of mass destruction. He previously worked with the Department of Energy as the site manager of the Andrews Air Force Base facility, responsible for one of the nation's Nuclear Emergency Search Teams. Mr. Moser later served as the Department of Homeland Security's (DHS's) protective security advisor to South Carolina, representing DHS as an onsite critical infrastructure and vulnerability assessment specialist. Mr. Moser

participated in comprehensive security assessments at nuclear power plants and material production facilities in North and South Carolina. Mr. Moser is an American Society of Industrial Security Certified Protection Professional and Physical Security Professional. He holds a B.S. in Business Administration from Waynesburg College in Pennsylvania, and an MBA from Southern Illinois University.

DAVID J. OSIAS is currently a consultant with Centra Technology, Inc. He retired in March 2008 as Chief of the Defense Intelligence Agency's (DIA's) Weapon Intelligence Group in the Directorate for Measurement and Signature Intelligence and Technical Collection. While at DIA, he had a broad range of responsibilities and gained extensive experience in intelligence analysis, much of it in technical areas relating to arms control, ballistic missiles, and weapons of mass destruction, particularly nuclear weapons. During his career, Dr. Osias led the postulated threat study, a Department of Defense (DOD) mandated recurring activity to inform decisions on physical security of U.S. nuclear forces. He was detailed twice to the Director of Central Intelligence, once to manage intelligence community activities to monitor and implement the Intermediate-Range Nuclear Forces treaty, and once to serve as national intelligence officer for strategic and nuclear programs. He also served in a rotational assignment as deputy director for intelligence and analysis in the Office of Intelligence of the Department of Energy. For his work on the INF treaty, Dr. Osias was awarded the DOD Distinguished Civilian Service Award. He has also been awarded Presidential Rank of Meritorious Executive, and has received two DIA director's awards. Dr. Osias received his B.S. in physics from the California Institute of Technology and his Ph.D. in nuclear science and engineering from Cornell University.

DANIEL M. SCHUTZER is chief technology officer, Technology Group, Financial Services Roundtable, since January 2010, an association of the 100 largest financial service companies plus affiliate members consisting of financial service technology vendors and service providers, national laboratories, universities, and government agencies, all aimed at addressing strategic business-technology issues, including security and information assurance for the financial sector. Prior to this, he was president of the Financial Services Technology Consortium (FSTC) division, Technology Group, Financial Services Roundtable from April 2005 to January 2010, where he brought broad perspective and depth to the consortium in leadership, technological impact on business systems and intelligence, and advanced systems in risk management and electronic commerce. Prior to joining FSTC, he served as a director and senior vice president of Citigroup with responsibilities ranging from trading to retail banking to security and corporate technology. Dr. Schutzer also served as the technical director of Naval Intelligence and Navy Command, Control, and Communications. He has also worked at Sperry Rand, Bell Laboratories, and IBM. He has authored over 65 publications and 7 books. Dr. Schutzer is a fellow of the New York Academy of Sciences. He served as a member of the National Research Council Committee on Critical Information Infrastructure Protection and the Law. Dr. Schutzer received his B.S.E.E. from the City College of the City University of New York and his M.S.E.E. and Ph.D. from Syracuse University.

BRIAN SNOW retired from the National Security Agency (NSA) in 2006 as technical director of the Associate Directorate for Education and Training and is currently an independent security consultant and ethics advisor. Mr. Snow has a broad-based competency in security technology, and particularly cryptographic systems design. He also has expertise in security protocols, intrusion detection systems, and security assessments and evaluations as applied to confidentiality, integrity, authenticity, availability, nonrepudiation, key management, network security, and information security systems. Mr. Snow spent his first 20 years at NSA performing and directing research that developed cryptographic components and secure systems, including Nuclear Command and Control systems. Computer security and network

security were major aspects for these systems. His later years at NSA were spent as a senior technical director in the Research Directorate (1994–1995); the Information Assurance Directorate (1996–2002), and the Directorate for Education and Training (2003–2006). Mr. Snow received an M.S. and a B.S. from the University of Colorado, both in mathematics.

FRANCIS X. TAYLOR is vice president and chief security officer for the General Electric Company (GE). He joined GE on March 7, 2005. He is responsible for overseeing GE's global security operations and crisis management processes. Prior to joining GE, Ambassador Taylor had a distinguished 35-year career in government service, where he held several senior positions managing investigations, security, and counterterrorism issues. Most recently, he served as the assistant secretary of state for diplomatic security and director of the Office of Foreign Missions, and oversaw all Department of State security programs that protect U.S. government employees and buildings overseas from terrorist, criminal, or technical attack and ensure the integrity of classified national security information produced and stored in those facilities, as well as protecting the secretary of state and foreign dignitaries who visit the United States. Ambassador Taylor also served as the U.S. ambassador at large and coordinator for counterterrorism for the Department of State from July 2001 to November 2002. In this role, he was responsible for the implementing U.S. counterterrorism policy overseas and coordinating the U.S. government response to international terrorist activities. During his 31 years of military service, Ambassador Taylor served with distinction in numerous command and staff positions, rising to the rank of brigadier general in September 1996. In his final active duty assignment, Brigadier General Taylor headed the Air Force Office of Special Investigations, where he was responsible for providing commanders of all Air Force activities with independent professional investigative services in fraud, counterintelligence, and major criminal matters. Mr. Taylor has received numerous awards and decorations, including the Distinguished Service Medal, the National Intelligence Distinguished Service Medal, the Defense Superior Service Medal and the Legion of Merit, and the Department of State Distinguished Honor Award. The University of Notre Dame Alumni Association honored his military service with the Father William Corby Distinguished Military Service Award. Mr. Taylor received his bachelor's and his master's degrees in government and international studies from the University of Notre Dame, and received his Air Force commission as a Distinguished Graduate of the Notre Dame ROTC program.

MARY D. ZALESNY is a behavioral and social scientist with the National Security Directorate at Pacific Northwest National Laboratory. She has over 25 years of research, teaching, and consulting experience in organizational and group behavior. Her research and professional experience include both basic and applied research in leadership and group behavior and processes, human judgment and information processing, networks (terrorist and social) and networked organizations, insider threat, and cyber and nuclear security. Analytic tools applied in the research and project work include social network analysis, statistical analysis (univariate and multivariate), network analysis, red team assessments, survey and test evaluation development, administration and analysis, and scenario development, among others. Her recent research has included ongoing technical support to the Department of Defense, Joint Chiefs of Staff, on behavioral and organizational issues related to terrorism and insurgencies; serving as a member of the U.S. Department of Energy (DOE) National Nuclear Security Administration team to identify insider threat issues at facilities storing and/or using radioactive materials for the Global Threat Reduction Initiative; serving as behavioral technical lead on a study of the insider threat for the Counterintelligence Field Activity; and advising the DOE's Radiological Dispersion Device (RDD) project (now Radiological Threat Reduction) on the social and psychological impacts related to RDD events. Dr. Zalesny received a B.S. in psychology and an M.A. and Ph.D. in industrial/organizational psychology from the University of Illinois at Urbana.

Appendix A: Statement of Task

The National Academies will advise the Department of Energy (DOE) on the augmentation of its current risk-based approach, the Design Basis Threat, for securing the nuclear weapons complex, specifically for securing nuclear weapons usable materials and facilities. The study will examine the augmentation of cyber security as well, while recognizing that cyber security and physical security present different challenges. The National Academies will:

1. Evaluate the potential applicability and feasibility of risk-based approaches, including probabilistic approaches, for securing the DOE nuclear weapons complex and document their potential strengths and weaknesses, cost effectiveness, and impediments to implementation. As part of this task, the National Academies will consider the experiences of DOE and its national laboratories, other federal agencies (e.g., Department of Defense, Department of Homeland Security, Nuclear Regulatory Commission), and the private sector (e.g., nuclear power industry) on the use of risk-based approaches for securing complex technological systems.

2. Evaluate whether and how dissuasion (i.e., deterrence and prevention) concepts can be incorporated into risk-based approaches to enhance security, both in terms of effectiveness and cost efficiency.

3. Provide practical and actionable findings and recommendations on the use of risk-based approaches to (i) balance physical and cyber security; and (ii) communicate within the government and with the public about security risks and costs.

Appendix B: Acronyms

DBT	design basis threat
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
GSP	Graded Security Protection Policy
HEU	highly enriched uranium
PRA	probabilistic risk assessment
SNM	special nuclear material