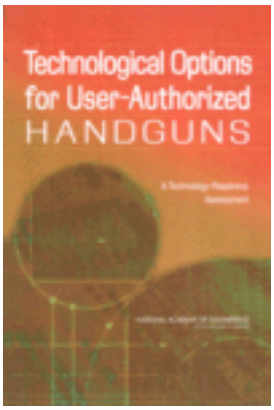


Technological Options for User-Authorized Handguns: A Technology-Readiness Assessment

Committee on User-Authorized Handguns
ISBN: 0-309-55190-0, 80 pages, 6 x 9, (2005)

Technological Options for User-Authorized HANDGUNS

A Technology-Readiness Assessment

Committee on User-Authorized Handguns

NATIONAL ACADEMY OF ENGINEERING
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: To arrive at the findings and recommendations of this report, the National Academy of Engineering has used a process that involves careful selection of a balanced and knowledgeable committee, assembly of relevant information, and peer review of the resultant report. Over time, this process has proven to produce authoritative and balanced results.

This study was supported in part by Grant No. 2002-24405 between the National Academy of Sciences and The David and Lucile Packard Foundation. 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 0-309-09699-5

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. Wm. A. Wulf 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. Wm. A. Wulf are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON USER-AUTHORIZED HANDGUNS

LANCE A. DAVIS (NAE) *chair*, National Academy of Engineering
LOUIS F. BEHLING, Picatinny Arsenal (retired)
RICHARD L. COSTELLO, Colt's Manufacturing Co. (retired)
T. DIXON DUDDERAR (NAE), Lucent Technologies (retired)
LAWRENCE O'GORMAN, Avaya Laboratories
LAWRENCE C. KRAVITZ, Allied Signal (retired)
DAVID MAHER, InterTrust
KAREN W. MARKUS, Zeus Strategies, LLC
JAMES J. MATTICE, Universal Technology Corporation
LAURENCE C. SEIFERT (NAE), AT&T Wireless (retired)
MARVIN H. WHITE (NAE), Lehigh University

Project Staff

GREG PEARSON, Program Officer, National Academy of Engineering (NAE)
RAY NASH, Consultant
CAROL R. ARENBERG, Managing Editor, NAE

Preface

This report is the final product of the Committee on User-Authorized Handguns, a group of experts on diverse subjects under the auspices of the National Academy of Engineering (NAE). The committee's charge included examining the state of the art of technologies that might be used in the design of a reliable user-authorized handgun (UAHG) and estimating the costs and time required to achieve that goal. The project builds on a 2002 NAE workshop that touched on technical and non-technical issues associated with the development of a UAHG.

In order to make the task more manageable, the committee focused its analysis on two groups of users: those in law enforcement and those who store and intend to use their firearms at home. The choice to frame the problem in this way was motivated by the committee's consideration of design constraints. In the law enforcement case, the firearm may have to operate in a variety of adverse conditions (e.g., involving cold temperature, water, mud, blood), which raises the bar significantly in terms of engineering challenges. In the case of homeowners, the requirements, while still imposing, are less difficult since such firearms would be used in relatively "clean" and uniform environmental conditions. There are, of course, many other categories of handgun user—for example, target shooters and individuals who possess a concealed-carry permit. In most of these cases, the technical requirements will align with those for law enforcement.

The committee hopes its report will inform ongoing discussions about the feasibility of developing handguns that may be less likely than standard-design firearms to be misused. Neither the report nor the committee takes a position regarding the desirability of producing a reliable UAHG.

Lance Davis, *chair*
Committee on User-Authorized Handguns

Acknowledgments

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 National Academy of Engineering. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to 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 wish to thank the following individuals for their review of this report:

Steven M. Bellovin, Columbia University
Kevin G. Foley, Smith & Wesson
Kenneth D. Green, Sporting Arms and Ammunition Manufacturers' Institute
David Hemenway, Harvard School of Public Health
E. Dan Hirleman, Purdue University
William F. Parkerson, III, National Rifle Association
Edward Polkowski, American Competitiveness Institute
Charles F. Wellford, University of Maryland
John W. Wirsbinski, Sandia National Laboratories

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the findings nor did they see the final draft of the report before its release. The review of this report was overseen by Dale F. Stein, Michigan Technological University (emeritus). Appointed by the NAE president, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

In addition to the reviewers, the committee wishes to extend special thanks to the following individuals who provided particularly helpful input to the committee: Kevin Foley, Smith & Wesson; Donald Sebastian, New Jersey Institute of Technology; Ed Schmitter, FN Manufacturing Inc.; Christopher Miles, National Institute of Justice; Bert Moore, Association for Automatic Identification and Mobility; Larry Keane, National Shooting Sports Foundation; and Mark Behrens, Esq., Shook, Hardy & Bacon, L.L.P.

Contents

Executive Summary

Misuse of handguns is a significant factor in deaths, morbidity, and crime in the United States. One approach to reducing certain types of handgun misuse is to create a user-authorized handgun (UAHG), a firearm that can be operated only by an authorized user(s). For the past decade, a handful of gun manufacturers, several university research groups, and a number of private research and development (R&D) groups have been exploring potential technologies for such a weapon.

The majority of this research, funded by the federal government through the National Institute of Justice (NIJ), part of the U.S. Department of Justice (DOJ), has been focused on the needs of the law-enforcement community. The level of investment has been modest, however, given the engineering challenges associated with developing a reliable UAHG. The total, including federal and state support, has been less than $12 million,[1] much of it for very preliminary proof-of-concept research. Gun manufacturers have spent very little of their own money on this research, and, at this time, NIJ has no plans to support additional research.

In 2002, the National Academy of Engineering (NAE) sponsored a one-day workshop that touched on three topics: the status and potential of

[1]All but $1million, which was provided by the New Jersey Legislature to the New Jersey Institute of Technology, has come from federal sources, either through a grant program at the National Institute of Justice or by direct congressional earmark.

technologies for UAHGs; the impact of UAHGs on public health and crime; and liability issues (NAE, 2003). In spring 2004, NAE formed the Committee on User-Authorized Handguns, whose members include research engineers, experts in manufacturing, and individuals experienced in handgun design and testing, to conduct the current study, which is focused exclusively on the technical aspects of developing a UAHG. This study is funded in part by a grant from The David and Lucile Packard Foundation.

GOAL AND OBJECTIVES

The goal of this project is to clarify the technical challenges of developing a reliable UAHG. The goal has four specific objectives:

Objective 1. Determine the **requirements** (e.g., reliability, environmental constraints, multiple-user capability) of UAHGs for two classes of owner: (1) people responsible for public safety (i.e., law-enforcement personnel); and (2) people concerned with personal safety and handgun misuse, particularly by children, in the home (i.e., homeowners).[2]

Objective 2. Based on these requirements, determine the **specifications** for UAHGs (e.g., time and ease of arming, time and ease of defeating the mechanism, definition of the fail-safe mode, size, weight).

Objective 3. Determine which **technologies** can satisfy the requirements and specifications among existing technologies, extensions of existing technologies, and new technologies that could be available in a reasonable time frame.

Objective 4. Assess the manufacturability and costs of the most promising technologies and estimate when they might become available commercially ("technology-readiness assessment").

[2]The committee recognizes that there are a number of non-law-enforcement user groups in addition to homeowners, including hunters, target shooters, collectors, and those with permits to carry concealed weapons. To the extent that these groups or homeowners wish to use or transport a handgun outside the home and want the ability to use it under adverse environmental conditions, the "homeowner" UAHG as we define it would not be suitable. Rather, the technical requirements for such firearms are likely to be similar if not identical to those for law enforcement.

REQUIREMENTS AND SPECIFICATIONS

In addressing the first two objectives, the committee relied heavily on work conducted by Sandia National Laboratories (SNL, 1996, 2001). The Sandia studies addressed only the needs of those concerned with public safety (i.e., law enforcement). The researchers surveyed the law-enforcement community to ascertain their requirements for a UAHG and translated a number of these general requirements into detailed "specifications." Although all of the requirements and specifications are important, the committee placed the highest priority on three vital categories—reliability, failure mode, and authentication.

AVAILABLE TECHNOLOGIES

In addition to the basic structure of the gun body, two critical kinds of technology must be part of any UAHG: (1) the authentication system and (2) the technology that permits or prevents firing of the weapon. For authentication to work, the gun user must have a unique identifier recognized by the handgun. The committee considered two classes of authentication technology—biometrics and token-based systems. Although at least a dozen biometric-based recognition technologies are being investigated for all kinds of systems, at this time only five (fingerprint, voice recognition, skin texture, skin spectroscopy, and handgrip pressure) are potentially appropriate for UAHGs. Of these, only two are being adapted for handguns: skin spectroscopy (by Smith & Wesson [S&W]) and handgrip pressure (by the New Jersey Institute of Technology [NJIT]).

Only one token-based technology (based on radio-frequency identification [RFID]) is in development for a UAHG at the present time. RFID systems generally consist of readers and transponders; each transponder (called an RFID tag) is associated with an entity to be identified. Transponders may be attached to, embedded in, or in proximity to the entity to be identified. If embedded, the tag becomes a "virtual biometric" that is permanently or semi-permanently associated with an individual. FN Manufacturing is working on a system with the Verichip (which has been approved by the Food and Drug Administration), an RFID tag that can be embedded under the skin (Applied Digital Solutions, 2004). The committee concluded that only embedded tags are appropriate for UAHGs.

Whichever authentication mechanism is used, it must interface with a latching mechanism on board the gun. Presently, handguns have

mechanical latching mechanisms that cock and release the hammer, which drives the firing pin into the primer. Gun companies have considerable competence and experience in designing latching systems. This does not mean, however, that engineering and production of the latching mechanism is simple. First, handguns require precision manufacturing to be reliable. Second, they are very compact, which means they have limited clearances for the addition of new electromechanical mechanisms to drive the latch. An alternative to an electromechanical latching mechanism is an all-electronic firing mechanism, which requires a special primer. This technology exists and has been used both commercially (in a rifle) and experimentally (in a prototype handgun by S&W). The choice of authentication technology will affect the failure mode of the firearm independent of latching/firing technology. An all-electronic handgun that loses electrical power to its authentication scheme can fail in the disarmed or armed mode, because power can still be available for firing.

TECHNOLOGY-READINESS ASSESSMENT

Neither the S&W skin-spectroscopy nor the NJIT handgrip-pressure authorization technology has reached the level of discrimination required either for the law enforcement community or homeowners. Both technologies are at a breadboard stage;[3] although the sensor is in a realistic configuration in the gun, the electronics for the reader are still external to the gun.

In judging the maturity of the technological components of a UAHG, the committee relied on a scale of technology-readiness levels (TRLs)[4] used by the National Aeronautics and Space Administration and the U.S. Department of Defense to gauge the maturity of technologies in development (GAO, 1999). Based on this rating system, the committee believes both the skin-spectroscopy and handgrip-pressure technologies are at TRL 4.[5]

---

[3]Technology at the breadboard stage of development replicates the function but not the configuration of the operational system and is not suitable for field testing.

[4]In the rating system used by the committee, technology readiness levels (TRLs) range from TRL 1 (observation of basic principles) to TRL 9 (actual application of the technology in its final form and under "mission" conditions).

[5]At TRL 4, component and/or breadboard validation is conducted in a laboratory environment. Basic technological components are integrated to establish that the pieces work together. The fidelity of the integration is relatively low compared to integration of the final system.

Because RFID systems are being developed for other applications, such as access control, they have reached a considerable level of maturity. Tag technology is highly developed, and even the embedded RFID sensor, which involves more complexity, has reached TRL 7[6] or TRL 8.[7] However, most current applications of RFID systems do not require miniaturization of the reader. Because considerable technology development will still be necessary to fit the reader electronics into the gun, the commmittee believes the integrated RFID reader for a UAHG is currently at TRL 5[8] or lower.

Some people in the gun industry believe that modifying the mechanical latching system by introducing an electronic interface may compromise the weapon's reliability. Nonetheless, FN Manufacturing has chosen to take the mechanical latch approach. Although an electromechnical latch may not be the most elegant solution, at this point in time, the committee believes such a latching scheme could be brought to TRL 6[9] in relatively short order, if FN has not done so already.

With respect to electronic firing, S&W has reported firing 60,000 rounds of electronically activated ammunition with prototype weapons with no reliability or power-source limitations (Kevin Foley, S&W, personal communication, 4/20/05). The firing electronics were fully integrated into the gun, and based on S&W's reported testing, the committee judges that this implementation of an electronic firing mechanism is at least at TRL 6, and possibly TRL 7.

---

[6]At TRL 7, system prototype is demonstrated in an operational environment. The prototype is near or at the planned operational system level.

[7]At TRL 8, an actual system is completed and "flight qualified" through testing and demonstration. Technology has been proven to work in its final form and under expected conditions. In almost all cases, TRL 8 represents the end of true system development.

[8]At TRL 5, component and/or breadboard validation is conducted in a relevant environment. Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment.

[9]At TRL 6, system/subsystem model or prototype is demonstrated in a relevant environment (sometimes called a brassboard model). A representative model or prototype system, which is well beyond the breadboard system tested for TRL 5, is tested in a relevant environment. This level represents a major step up in demonstrated readiness.

Metal Storm, an Australian defense research company, has explored a radically different design for an electronically fired handgun in which the projectiles are stacked in the barrel and fired in sequence. NJIT has entered a partnership with Metal Storm with the hope of integrating its grip-pressure recognition technology into the new handgun design (NJIT, 2003). However, because this is a rather new concept and even the ammunition will require a development project, the committee judges that this technology could be anywhere from TRL 3[10] to TRL 5.

CONCLUSION

Developing a UAHG for law enforcement poses serious engineering challenges: the need for a very low false-rejection rate and the need for the firearm to function in inclement environmental conditions, high-stress situations, in the presence of dirt, and with users who might wear gloves. In terms of the likelihood of successful development, both the skin-spectroscopy and handgrip-pressure technologies under development are unproven, high-risk technologies. RFID sensing appears to be a relatively low-risk technology, in the sense that it has an extensive and well documented track record in other applications. But, like biometric sensors, it would require miniaturized components in the gun, which is not a trivial undertaking.

Even a UAHG for homeowners, who may have less daunting authentication requirements, poses significant technical challenges. Inclement weather, dirt, and gloves would not be significant factors, but the need for recognition of an authorized user in a stressful situation would be just as demanding for the authentication sensor, and the gun should share the requirement of a law enforcement gun of being extremely difficult for an unauthorized person intentionally to bypass the security system by whatever means possible. However, if the emphasis is placed on the rejection of an unauthorized user, especially a child, the demands on the sensor are likely to be somewhat less stringent than for law enforcement. In this case, the product designer must chose between the "perfect" solution and the "good" solution.

[10] At TRL 3, analytical and experimental critical functions are identified and/or characteristic proofs of concept are developed. Active R&D is initiated, including analytical studies and laboratory studies to validate analytical predictions of separate elements of the technology.

Developing a reliable UAHG will require technologies that are beyond the experience base of gun companies. And, that experience base has kept the development costs of conventional guns fairly low. Through the NIJ program, S&W, FN Manufacturing, and NJIT have each already spent, or will soon have spent, amounts approaching the development cost of a conventional gun (on the order of $3 million to $4 million; see Appendix D) and, in the committee's judgment, all of them are still a long way from having developed integrated brass-board test articles[11] (i.e., TRL 5 devices), even though individual component technologies may be more mature. In addition, the monies spent to this point are early-stage costs; typically, absent an experience base, development costs escalate rapidly at this point. The committee estimates that total costs to bring a single implementation of a UAHG to market could easily reach several times to as much as 10 times what each developer has spent to date, or on the order of $30 million, particularly for a version that uses true biometric authentication and could take 5 to 10 years to complete. If one were to start anew, with present developments as the baseline, the committee suggests that the shortest path to success, with cost and time at the lower ends of these ranges, would involve a mechanical or electronic gun interfaced with an RFID tag inserted under the skin. Recent progress in the development of a UAHG has been almost solely the result of research funded by NIJ. However, there is no follow-on funding in the 2005 fiscal year federal budget for this program (Christopher Miles, NIJ, personal communication, 9/13/04). The committee is not aware of any substantive developments outside the NIJ program and expects the present development efforts to come to an end if and when NIJ funding is exhausted.

REFERENCES

Applied Digital Solutions. 2004. Verichip Corporation enters into a memorandum of understanding for the development of a firearm's user authorization system—"Smart Gun"—using Verichip RFID technology. Press release. Available online at: *http://www.adsx.com/news/2004/041304.html* (February 13, 2005).

[11]Technology at the brassboard stage of development replicates both the function and configuration of the operational systems with the exception of non-essential aspects such as packaging and can be field tested. A brass board is more advanced in development than a breadboard.

GAO (General Accounting Office). 1999. Best Practices: Better Management of Technology Development Can Improve Weapon System Outcomes, edited by L. Rodrigues and P. Francis. GAO/NSIAD-99-162, July, 1999. Washington, D.C.: General Accounting Office. Available online at: *http:/www.gao.gov/archive/1999/ns991620.pdf.*

NAE (National Academy of Engineering). 2003. Owner-Authorized Handguns: A Workshop Summary, edited by L.A. Davis and G. Pearson. Washington, D.C.: National Academies Press.

NJIT (New Jersey Institute of Technology). 2003. New Jersey Institute of Technology moves ahead to get smart gun on market. Press release, September 5, 2003. Available online at *http://www.njit.edu/v2/News/Releases/395.html.* (April 20, 2005)

SNL (Sandia National Laboratories). 1996. Smart Gun Technology Project Final Report, edited by D.R. Weiss. SAND-96-1131. Available from National Technical Information Service, Springfield, Va. NTIS Order Number: DE96013854.

SNL. 2001. Smart Gun Technology Update, edited by J.W. Wirsbinski. SAND-2001-3499. Available from National Technical Information Service, Springfield, Va. NTIS Order Number: DE2001-789587.

Technological Options for User-Authorized Handguns

Misuse of handguns is a significant factor in crime, accidents, suicides, and morbidity in the United States. In recent years, some have looked to advances in technology for a user-authorized handgun (UAHG) to address this problem.[1] The idea behind a UAHG is that the weapon "recognizes" the owner(s) or other authorized user(s) and can only be fired when that individual(s), and no one else, wants the gun to fire. A variety of sensor, electronic, mechanical, and other technologies might be used in the design of such a weapon.

A basic tenet of gun ownership and use is "reliability," that is, a gun must fire when an owner wants it to fire and must not fire otherwise. A UAHG must be as close to 100 percent reliable as possible. A successful UAHG design will have to pass a number of hurdles to meet the reliability criterion. For instance, in law enforcement and self-defense situations, the gun must be able to be armed quickly for firing, but an unauthorized person(s) in close proximity to the owner must not be able to fire it. In addition, a UAHG must be designed to take account of the possible failure

[1]User-authorized guns are sometimes called "smart" guns or personalized guns. In this report, we generally use the term "user-authorized gun (UAHG)," which both avoids the personification implied in the "smart gun" label and recognizes that guns may have more than one intended user.

of the embedded technology (i.e., it must have an appropriate fail-safe mode).

The National Academy of Engineering (NAE) (www.nae.edu), part of the National Academies (www.nationalacademies.org), is a nonprofit organization that leverages the expertise of its members and others to explore important topics in engineering and technology that have significant economic or social implications. As part of a strategic planning effort that began in 2000, the NAE Council directed the NAE Program Office to examine a number of issues of significant public interest, including UAHGs. For the most part, the feasibility of developing a UAHG has not been informed by sound, objective technical or scientific analysis. NAE's purpose is to perform a public service by providing an unbiased review of the issue.

Over the past decade, the U.S. Department of Justice (DOJ) National Institute of Justice (NIJ), some gun manufacturers, several educational and private institutions, and private inventors have addressed the issue of UAHGs. Beginning in fall 2000, NAE staff began to collect and read existing reports on the topic and to talk with a number of knowledgeable individuals in the gun industry, law enforcement, public health, and other sectors. This exploratory phase culminated in a one-day NAE-funded workshop on June 7, 2002, in Washington, D.C. The workshop focused on three issues: the status and potential of technologies for UAHGs; the possible impact of UAHGs on public health and crime; and product liability concerns. (See Appendix A for a copy of the workshop agenda.) A workshop summary report was published in 2003 (NAE, 2003).

The current project, a continuation of NAE's exploration of the UAHG issue, is focused specifically on the technical dimensions of developing and producing such a firearm. In spring 2004, NAE formed the Committee on User-Authorized Handguns, whose members have expertise in a wide range of relevant disciplines and professional fields. (See Appendix B for a committee roster.) The current project was partially funded by a grant from The David and Lucile Packard Foundation.

GOAL AND OBJECTIVES

The goal of this project is to clarify the technical challenges of developing a reliable UAHG. The goal has four specific objectives:

Objective 1. Determine the owner **requirements** (e.g., reliability, environ-

mental constraints, multiple-user capability) of UAHGs for two classes of gun users: (1) those concerned with public safety (e.g., law-enforcement personnel); and (2) those concerned with personal safety (e.g., homeowners protecting themselves and their property).[2]

Objective 2. Based on the requirements, determine the **specifications** for UAHGs (e.g., time and ease of arming, time and ease of defeating the mechanism, definition of fail-safe mode, size, weight, etc.).

Objective 3. Identify **technologies** that could satisfy the requirements and specifications. The committee focused specifically on existing technologies, extensions of existing technologies, and new technologies that could be available in a reasonable time frame.

Objective 4. Assess the manufacturability and costs of the most promising technologies and estimate when they might become available commercially (**technology-readiness assessment**).

DATA GATHERING

The committee gathered information for its assessment from a variety of sources. In addressing Objectives 1 and 2 (requirements and specifications), the committee relied heavily on work by other groups. The first of two reports from Sandia National Laboratories, *Smart Gun Technology Project Final Report* (SNL, 1996), was particularly helpful. This report includes the results of a comprehensive survey of the needs of the law-enforcement community and rates the potential of technologies available at the time to meet those needs. The second Sandia report, an update of the first, draws the same general conclusions (SNL, 2001). In addition, the committee reviewed a 2001 report by the New Jersey Institute of Technology (NJIT). Few other documents address the technical aspects of UAHGs.

[2]The committee recognizes that there are a number of non-law-enforcement user groups in addition to homeowners, including hunters, target shooters, collectors, and those with permits to carry concealed weapons. To the extent that these groups or homeowners wish to use or transport a handgun outside the home and want the ability to use it under adverse environmental conditions, the "homeowner" UAHG as we define it would not be suitable. Rather, the technical requirements for such firearms are likely to be similar if not identical to those for law enforcement.

To address Objectives 3 and 4, the committee spoke informally and formally with representatives of the gun industry and academic researchers involved in research and development (R&D) on UAHGs. Several individuals met face-to-face with the committee to discuss their past and current work in this area. The committee also was given a briefing by the staff at NIJ, the source of federal funding for R&D on UAHGs. To ensure that the entire landscape of possible technological approaches for UAHGs had been considered, the committee reviewed the database of the U.S. Patent and Trademark Office for relevant patents and patent applications. This review revealed that, although a number of patents suggest designs for UAHGs, the vast majority of patents are owned by individuals as opposed to companies. Overall, the committee found few ideas for personalizing handguns that were not described in the Sandia or NJIT reports. The few patents that could be linked directly to gun manufacturers were for designs already known to the committee.

Because the goal of the project was not to look into highly speculative technologies or to "design" a wholly new approach to the creation of a UAHG, the committee decided to focus on a limited number of technologies and their implementation, or potential implementation, in a UAHG. These technologies "span the space" of the two classes of users and handgun technologies and, in effect, represent the "survivors" of the larger number of technologies reviewed in the Sandia and NJIT reports.

TECHNOLOGY-READINESS LEVELS

Based on the handgun designs/technologies chosen for consideration and available public information, the committee made technology-readiness assessments, based on a rating system used by the National Aeronautics and Space Administration, U.S. Department of Defense, and others to gauge the maturity of technologies in development (GAO, 1999). The system defines nine technology-readiness levels (TRLs) (Box 1).

HANDGUNS AND RESEARCH IN CONTEXT

Between 1899 and 2000, U.S. gun manufacturers produced some 217 million guns, 76 million of them handguns, according to federal data collected by the Violence Policy Center (2002). Handgun production topped 1 million annually for the first time in 1968 and has remained above that level ever since.

The peak year for handgun production was 1993, when 2.8 million were manufactured. In 2003, the most recent year for which data are available, American gun manufacturers produced 1.12 million handguns (BATF, 2005). Handguns historically have accounted for one-third of all guns made in this country. About 80 percent of the guns available in the United States are manufactured here (BJS, 1995).

According to the most recent federal data, in 2001 a total of 29,342 people were killed by handguns; 57 percent of these deaths were suicides (Vyrostek et al., 2004). There were 802 unintentional firearm-related deaths that year, and 56,697 people were injured by handguns, nearly two-thirds in assaults. In 1994, the lifetime medical costs of treatment of gunshot injuries in the United States was estimated at $2.3 billion, $1.1 billion of which was paid by the federal government (Cook et al., 1999).

Although most crimes are not committed with guns, nearly 90 percent of gun crimes are committed with handguns, and of the roughly 300,000 guns stolen each year, slightly more than half are handguns (BJS, 1995). In 2003, perpetrators of 25 percent of robberies, 7 percent of violent crimes, and 3 percent of rapes and sexual assaults used firearms (BJS, 2004). Studies of adult and juvenile offenders reveal that many of these individuals (between 10 and 50 percent, depending on the study) have stolen a handgun or sold or traded a stolen handgun (e.g., NIJ, 1993).

Handguns are often fired by persons other than their owners or other authorized users. Criminals frequently use stolen handguns to commit burglaries and robberies. Handguns are the weapons of choice for people who decide to kill themselves, and in many cases they use weapons obtained from family members or friends. A police officer's handgun may be taken and fired by a suspect during a struggle or used later to commit a crime. According to the Federal Bureau of Investigation (2003), in the 10-year period between 1994 and 2003, 616 police officers were killed in the line of duty, including 50 who were slain by an adversary using the officer's own weapon. The number of officers killed with their own weapons has declined from about 15 per year in the 1980s to about 5 per year for the last 15 years. This decline is believed to be due in part to the use of retention holsters and body armor, improved trauma care, and "take-away" training (Christopher Miles, NIJ, personal communication, 9/13/04). Tragically, young children sometimes find and accidentally discharge handguns, injuring or killing themselves or others. In 2001, 72 children aged 14 or younger were accidentally killed by firearms (Vyrostek et al., 2004).

The primary method of preventing accidental firearm-related deaths

BOX 1
Technology-Readiness Levels[a]

TRL 1. Basic principles are observed and reported. Scientific research begins to be translated into applied R&D. Examples might include paper studies of the basic properties of a technology. This is the lowest level of technology readiness.

TRL 2. Technology concept and/or application has been formulated, and invention of practical applications has begun. Applications are speculative, and there are no proofs or detailed analyses to support assumptions. Examples are still limited to paper studies.

TRL 3. Analytical and experimental critical functions are identified and/or characteristic proofs of concept are developed. Active R&D is initiated, including analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.

TRL 4. Component and/or breadboard[b] validation is conducted in a laboratory environment. Basic technological components are integrated to establish that the pieces work together. There is relatively low fidelity compared to the final system. Examples include the integration of "ad hoc" hardware in a laboratory.

TRL 5. Component and/or breadboard validation is conducted in a relevant environment. Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components.

TRL 6. A representative system/subsystem model or prototype (sometimes called a brass-board model), which is well beyond the breadboard system tested for TRL 5, is tested in a relevant environment. This level represents a major step up in demonstrated readiness. Examples include testing of a prototype in a high-fidelity laboratory environment or in a simulated operational environment.

TRL 7. A system prototype is demonstrated in an operational environment. The prototype is near or at the planned operational system level. This level represents a major step up from TRL 6 because it requires the demonstration of an actual system prototype in an operational environment, such as in an aircraft, a vehicle, or space. Examples include testing of a prototype in a test-bed aircraft.

TRL 8. An actual system is completed and "flight qualified" through testing and demonstration. Technology has been proven to work in its final form and under expected conditions. In almost all cases, TRL 8 represents the end of true system development. Examples include developmental testing and evaluation of a system in its intended operational setting to determine if it meets design specifications.

TRL 9. An actual system has been "flight proven" through successful mission operations. The technology has been applied in its final form and under mission conditions, such as those encountered in operational testing and evaluation. In almost all cases, this is the end of the last "bug fixing" aspects of true system development.

---

[a]The committee notes that TRLs are not intended to account for production readiness or cost. Although the fidelity of the test environment increases from TRL 7 through TRL 9, this testing does not require that an article (or representative lot runs) be manufactured with production tooling, processes, or quality controls. The committee considered this when assigning TRLs to specific UAHG technologies.

[b]Technology at the breadboard stage of development replicates the function but not the configuration of the operational system and is not suitable for field testing.

SOURCE: Adapted from GAO, 1999.

or injuries to minors has been to encourage gun owners to store and handle handguns properly. Storage methods include placing guns in a safe or rendering them otherwise physically inaccessible, using any of a variety of mechanical locks intended to keep guns from firing, and storing guns unloaded with the ammunition and guns in separate locations. Gun owners can also take courses in firearms safety, where they are taught and can practice safe procedures for loading, unloading, and firing handguns. Unfortunately, however, safety procedures are not always followed.

Trigger locks and other simple methods of preventing the unintentional firing of guns have been available for decades. Only recently have more sophisticated, technological fixes been the subject of investigation. According to one recent review of the literature, there currently are insufficient data to determine how the introduction of UAHGs into the marketplace might affect handgun-related injuries and deaths (NRC, 2005).

Researchers at Sandia National Laboratories, funded by NIJ, conducted perhaps the first substantive assessment of the state of the art in UAHG technology (SNL, 1996). The study included the results of a comprehensive survey of law-enforcement personnel to determine their requirements for a UAHG and a comparison of those needs with a range of technologies in existence at the time. (By charter, DOJ, of which NIJ is a part, can study handguns only in the context of law enforcement. However, the results of research funded by NIJ may be applicable to other gun users.) The study found that a number of technologies met at least some of the police officers' requirements, but there was no acceptable "smart-gun" technology. An updated study was published in 2001, again funded by NIJ (SNL, 2001).

In July 1999, the New Jersey legislature appropriated $1 million to NJIT for a review of current and emerging technologies that might be used to create a UAHG. The study was motivated in part by a bill then being considered by the legislature to require all handguns sold in the state to be "personalized" within three years after appropriate technology became commercially available. (The legislation has since become law.) The NJIT report (2001) concluded that the development of a UAHG was feasible and recommended that additional R&D be done on a specific biometric technology, handgrip-pressure recognition.

The first recipient of federal funds to pursue the development of UAHG technology was Colt's Manufacturing Company, which received $500,000 in 1998 to develop a gun with a magnetic-based key-recognition system. Colt abandoned its research on UAHGs in 2000. From 2000 to 2004, the NIJ program provided R&D support to two established

gun manufacturers, Smith and Wesson (S&W) and FN Manufacturing, and five research groups, Metal Storm, Mosermation, iGun, Technology Next, and Exponent (Table 1). (For brief summaries of these awards, see Appendix C.)

Many of these awards, as well as support for the 2001 update of the first Sandia report, were made possible by a one-time, $8 million congressional appropriation to NIJ for research on UAHGs. Those funds have now been expended, and NIJ does not plan to pursue the program beyond 2004. Congress also earmarked $1.1 million in 2004 and $1 million in 2005 for NJIT to conduct additional R&D on handgrip-recognition technology.

Since Colt abandoned its R&D, work done by S&W and FN Manufacturing represents the most advanced developments for a UAHG. NJIT, a rather recent entry in the field, formed partnerships (NJIT, 2003) with Metal Storm Ltd., an Australian company, and Taurus International Manufacturing Inc., a Brazilian company with an office in Miami, to exploit its handgrip-pressure identification technology (TIM, 2003). According to statements by the companies involved, Metal Storm has a patented electronic-ignition technology, and Taurus, which manufactures handguns and other products, had agreed to integrate the electronic ignition with NJIT's handgrip-pressure biometric in a commercially viable UAHG. However, in February 2005, Taurus announced its withdrawal from the partnership (Tartaro, 2005).

In addition to gun manufacturers, a number of other organizations and individuals have a stake, or may have a stake, in the development of a UAHG (Box 2).

Although all of these stakeholders have opinions about the desirability of the development of UAHGs, this report focuses largely on gun manufacturers and two user groups: law enforcement personnel and homeowners, individuals who store and intend to use their firearm at home. Law-enforcement officials use handguns to enforce the law, deter criminal activity, and protect themselves. Homeowners use handguns to protect their property, themselves, and their families. Both groups are concerned about preventing the accidental or purposeful misuse of their guns. Law-enforcement firearms kept at home may fall into the hands of an unauthorized family member, such as a child, just as easily as a handgun kept at home by someone not in law enforcement. Similarly, both law-enforcement officials and homeowners face the possibility of having their weapons taken from them in a struggle with an adversary. Despite these

TABLE 1 Summary of DOJ/NIJ Contracts for User-Authorized Handguns

Award Recipient	Approximate Dates	Approximate Funding	Description/ Comments
Sandia National Laboratories	1994–1996; updated in 2001 (see later entry)	$625,000	Identified technologies to address the police firearm take-away problem.
Colt's Manufacturing Company	1998–2000	$500,000	R&D on a UAHG with a fluctuating magnetic field. Project abandoned in 2000 for lack of follow-on funding.
Smith & Wesson (with Lumidigm, a subcontractor)	2000–2004	$3,673,000	R&D on hand-entered PIN, fingerprint identification (the latter now abandoned), and "tissue spectroscopy."
FN Manufacturing	2001–2003	$2,306,000	R&D on microelectronic and radio-frequency identification technologies.
Sandia National Laboratories	2000–2001	$70,000	Update previous report and survey commercial off-the-shelf technologies.

commonalities, because of the need to accommodate adverse environmental conditions, the technical requirements for a law-enforcement UAHG will be more stringent than for a homeowner firearm. This issue is discussed in greater detail in Objective 1: User Requirements, below.

LEGISLATIVE AND LIABILITY CONSIDERATIONS

New Jersey is the only state that has passed a law that addresses the issue of UAHGs directly. The New Jersey legislation, passed in December 2002, specifies that "three years after it is determined that personalized

TABLE 1 Continued

Award Recipient	Approximate Dates	Approximate Funding	Description/ Comments
Mosermation	2001–2004	$300,000	R&D on handgrip characteristics.
iGun	2002	$369,000	Study of biometric technologies.
Technology Next Inc.	2002–2003	$176,000	R&D on an authorization system for using radio-frequency coding technology.
Exponent Inc.	2002–2004	$188,000	R&D on an authorization system based on spectral characteristics of a compound (e.g., special ink).
Metal Storm/ VLe Small Arms	2002–2003	$185,000	R&D on a total electronic handgun.
New Jersey Institute of Technology	2004–2005	$2,130,000[a]	Further R&D on handgrip-pressure technology.

[a] Does not reflect a one-time appropriation of $1 million by the New Jersey legislature to the New Jersey Institute of Technology in 1999.

handguns are available for retail purposes, it will be illegal . . . for any dealer or manufacturer to sell, assign, or transfer any handgun unless that handgun is a personalized handgun" (New Jersey Code of Criminal Justice, 2C:58-2.2). Under the law, the state attorney general must assess the availability of such firearms every six months. The three-year clock begins to run once he or she determines that the technology is available at the retail level.

In 1997, the attorney general of Massachusetts promulgated consumer-safety regulations for guns sold in the state based on laws already on the books. According to the Brady Center to Prevent Gun Violence (2001),

BOX 2
Stakeholders in User-Authorized Handguns

Handgun Users

- the military services
- national, state, and local law-enforcement agencies
- private security officers
- homeowners
- gun collectors
- target shooters
- concealed-carry permit holders
- hunters
- criminals

Stakeholders with Direct Economic Interests

- handgun manufacturers
- manufacturers of technologies that might be used in UAHGs
- handgun retailers and wholesalers

Stakeholders with Indirect Economic Interests

- not-for-profit laboratories/firms and universities that assess technologies, develop prototype technologies and handguns, and might be involved in forming partnerships/consortia for the development and manufacture of UAHGs
- university criminal-justice departments[a]
- the legal community[a]
- health insurance companies

The Public

- state and federal government agencies
- public health entities and some foundations
- advocacy groups (e.g., National Rifle Association, Brady Campaign to Prevent Gun Violence)

---

[a] University criminal justice departments are stakeholders with indirect economic interests, because they may receive funding to study handgun-related issues. The legal community likewise has an indirect economic interest in handguns, because lawyers receive money for engaging in handgun-related litigation.

although these regulations do not require the personalization of handguns, similar consumer-safety laws in 20 other states could be used to impose such a mandate. At least one other state, Maryland, requires that an advisory board regularly review the status of personalized handgun technology and report its findings to the governor (Maryland Code § 5-132).

Product liability is likely to affect the development and sale of UAHGs. Liability may be based on three circumstances: (1) a manufacturing flaw that causes the product to fail to perform as intended; (2) a design defect, that is, an unsound design that makes the product unsafe when used as intended; and (3) failure to warn of a risk posed by the product. Liability generally may attach under these circumstances against the manufacturer of the product and against any downstream distributor or seller who participates in the stream of commerce. Liability issues may also affect suppliers of component parts.

Courts have generally been reluctant to use the theory known as "negligent marketing," that is, the products are so dangerous and offer so little benefit to society that they should not be sold at all, to hold manufacturers and sellers of handguns liable. In questionable situations, courts have declined to "regulate by litigation" and deferred to legislatures to decide whether handgun sales should be banned.

Because manufacturing flaws are rare with modern manufacturing and quality-control systems, and because manufacturers generally do warn buyers of potential risks regarding their products, most litigation involving UAHGs is likely to be based on design liability. According to one school of thought, handgun manufacturers that fail to incorporate user-authorization technology may be subject to design liability claims. (This is analogous to car manufacturers being held liable for not supplying air bags. By not supplying air bags, the argument goes, manufacturers would invite more litigation than might be incurred from improperly functioning air bags.)

To be successful, however, plaintiffs in most states would have to show that the risk of the product as sold outweighed the product's utility. These claims must overcome several legal hurdles. For example, a manufacturer cannot be required to incorporate a technology that renders the product substantially more expensive and, thus, less attractive to consumers.

Courts in states that use this "risk-utility" approach would also have to consider the benefit of the added cost in light of the limitations of UAHG technology. For instance, if the technology were to be based on fingerprint identification, the handgun may not have any utility for a person wearing a

glove in cold weather. Similarly, the product may lack utility for a law-enforcement officer wearing gloves to protect against abrasions during an arrest or to guard against exposure to a dangerous instrument, such as a knife, razor blade, or dirty needle. The product may also lack utility if an officer is downed and another officer has to pick up his or her gun to continue to engage a criminal. If the technology were based on a bracelet that emits a radio signal, the product may lack utility for a person forced to pull the handgun in the dark, since it might be difficult to find the bracelet quickly under those circumstances.

Some states do not use a "risk-utility" test to determine if products have defective designs. These states use a "consumer-expectations" test—did the product fail to meet the expectations of the ordinary consumer? Because most handguns sold today do not have user-authorization technology, a plaintiff would have trouble convincing a court that a handgun without such technology failed to meet the user's expectations.

If user-authorization technology would create a liability that otherwise might not exist, manufacturers are likely to be reluctant to spend potentially large resources on R&D to develop it. Thus, at least one gun manufacturer feels strongly that there must be some sort of "hold-harmless" legislation in place to limit liability before user-authorized technologies are developed and introduced into the marketplace (Kevin Foley, S&W, remarks made at a National Institute of Justice program review meeting, October 9, 2003, Washington, D.C.). The committee neither supports nor opposes the passage of any version of hold harmless legislation; it merely notes that resolution of the liability issue could be a prerequisite to the commercialization of UAHGs.

Because handguns, like most other products, are transported in interstate commerce, legislation providing incentives for the development and marketing of UAHGs would have to come from Congress to be effective on a national scale. Under current circumstances, legislation protecting a manufacturer from liability in one state would not be effective if the handgun were sold or an injury occurred in a different state.

An interesting point of reference is the Medical Device Amendments of 1976 to the Federal Food, Drug and Cosmetics Act. The amendments set forth a comprehensive scheme of federal legislation and regulation designed to maximize the safety attributes of medical devices while helping to insulate medical device manufacturers and suppliers from product liability suits that might otherwise cripple this important industry. Congress attempted to strike a balance with a "preemption" clause, the essence of which

is (somewhat simplified here) that no state can impose requirements on a product that differ from, or are in addition to, the requirements prescribed by federal law. In other words, claims that a product is defective because it failed to do (or be) something other than what the federal law required it to do (or be) are preempted, and the product liability claim must be dismissed as a matter of law.

OBJECTIVE 1: USER REQUIREMENTS

One of the first steps in product development is to determine the customer's needs. In engineering design, these needs are called "requirements." The committee believes that a UAHG that meets the physical and environmental requirements of law-enforcement personnel and homeowners would also meet the requirements of other users (hunters, target shooters, concealed-carry permit holders, and collectors). Therefore, this report focuses on the requirements of two classes of gun users: (1) gun users concerned primarily with public safety (i.e., law enforcement personnel); and (2) gun users concerned primarily with personal safety and protection of property in the home (e.g., homeowners).

Chapter 7 of the 1996 Sandia report (summarized in Appendix A of the 2001 Sandia update) provides an excellent starting point for defining handgun requirements. Based on interviews with police officers, Sandia researchers compiled a list of more than 70 requirements for a UAHG that would meet the needs of law enforcement personnel. The Sandia authors translated a number of these general requirements into more detailed "specifications." For example, officers were very concerned that they be able to draw a UAHG from a holster and fire it as quickly as a traditional firearm. The report authors suggest a target value, or specification, of 0.25 seconds from the time an authorized user grabs the gun and the time the gun can be fired.

The Sandia researchers organized the requirements into 20 categories (Table 2). Ideally, all of these requirements would be met in a handgun intended for law-enforcement applications. In practice, it is unlikely that every requirement can be satisfied in a single weapon. As in any engineered product, achieving a reasonable balance among the requirements will require trade-offs.

The committee recognized that the reliability of a UAHG is not simply related to the reliabilities of the firearm's conventional and unconventional components. The necessary integration of these mechanical and

TABLE 2 Requirements for a User-Authorized Handgun for Law Enforcement

Requirement	Number of Sub-requirements
Scope	4
Physical characteristics	4
Power	7
Operation	19
Key (the unlocking method/algorithm)	10
Discriminator (logic involved in reading the key)	10
Latch (physical mechanism activated by the discriminator)	5
Indicators (of enabled/disabled)	4
Documentation	3
Safety	2
Other Standards (NIJ/SAAMI)[a]	2
Adversarial strength (resistance to efforts to "defeat" the locking mechanism)	3
Training	2
Maintenance	7
Interface (upgrade capability)	3
Cost	3
Testing	3
Reliability	1
Service life	1
Environments	15

[a]SAAMI (www.saami.org), the Sporting Arms and Ammunition Manufacturers' Institute, develops voluntary standards for the safety and quality of firearms and ammunition.
SOURCE: SNL, 2001.

electronic elements may compound reliability issues. Because of this complexity, the committee consciously focused on the requirements of the user-authorization technologies at this early stage of product development.

There are three significant differences between the requirements for the public-security application and the personal-safety use of a UAHG. First, if the user-authorizing features of the gun fail to work for a police officer, either because of a malfunction or loss of power (if the firearm is powered by a battery), the gun should "fail" in an armed mode so it can still be fired. In contrast, if a UAHG malfunctions for a homeowner, the weapon

could be designed to fail in either a disarmed mode (so that it could not be picked up and used by an unauthorized person, particularly a child) or an armed mode (e.g., if no children live in the home or children visit only periodically). Second, there should be fewer requirements for environmental and performance testing for the homeowner's weapon than for the police officer's weapon. In general, firearms used by police officers are much more likely to be used in adverse conditions than those stored and used primarily in the home. Third, there appears to be little justification for a handgun stored and used in the home to accommodate a user wearing gloves. The committee wishes to emphasize, however, that despite the lower threshold for the homeowner's weapon, the requirements must still be stringent so the gun is not "unreasonably dangerous," thus opening the manufacturer to liability claims.

In any event, one can envision a UAHG that works successfully in a home-protection situation but may not be 100 percent satisfactory for a law-enforcement situation that involves adverse environmental conditions (e.g., rain, snow, mud, or blood) that may affect reliability. Similarly, a UAHG that is not fully satisfactory for defending against an intruder could still prevent an unauthorized person, such as a child, from unintentionally harming himself or herself or others. Such a gun might also be appropriate for use by a target shooter, who typically does not require rapid access. But limited access could also be ensured with a lock box, a mechanical trigger lock, or a disabling tie-down.

OBJECTIVE 2: SPECIFICATIONS

Requirements reflect how the user wants the product to function. **Specifications** quantify the requirements and define the parameters of the manufactured product. Based on its own judgment as well as information from the two Sandia reports, NIJ, and military handgun testing guidelines, the committee has compiled what it believes is a reasonable set of requirements and corresponding specifications for a UAHG (Table 3).

OBJECTIVE 3: AVAILABLE TECHNOLOGIES

The basic concept behind a UAHG is that an authorized user has an identifier that allows him (or her) alone to discharge the weapon. A general discussion of the concept of authentication is given below.

TABLE 3 Requirements and Specifications for User-Authorized Handguns

Reliability

- Gun fires 500 to 1,000 average rounds between failures (authorization at beginning of test sequence and failure due to loss of authorization or of firing mechanism).
- False reject rate[a] (FRR) is less than FAR and as close to 0 percent as possible.
- False acceptance rate[b] (FAR) is 5 percent or lower.

Failure Mode

- For law enforcement, if user-authorization system loses power or malfunctions, weapon fails in the armed or active mode.
- For homeowner use, if user-authorization system fails, the weapon fails in active or inactive mode, depending on the needs[c] of the gun owner.

Authentication[d]

- With authentication of authorized user, inoperable weapon moves to operable status.
- With attempted authentication of unauthorized user, operable weapon moves to inoperable status.
- Authentication (recognition by the discriminator) is accomplished in 0.25 seconds or less.
- Indicator shows whether the weapon is enabled or disabled.

Physical Characteristics

- The size, shape, weight, and balance are approximately the same as for existing pistols/revolvers.
  - no more than 3.5 oz added to weight
  - no more than 2 cubic inches added to volume

Ease of Compromise

- User-authorization features components, including software, are not easily spoofed or defeated.
- Attempts to spoof/defeat/destroy/remove user-authorization features render weapon permanently inoperable.

Use Scenarios

- UAHG can be used with either right or left hand of the same person and can be fired with one or two hands.
- For law enforcement, weapon can be used by individuals wearing gloves.
- Weapons for homeowners are not usable by individuals wearing gloves.
- Certain UAHGs are usable by more than one authorized individual.

TABLE 3 continued

Performance and Environmental Testing

- Weapon undergoes same test as traditional handguns to ensure that embedded microelectronics, batteries, and other components can withstand various types of use and abuse.
- For law enforcement, the following tests should be considered (for homeowners, less extensive testing may be necessary):
  - endurance testing (repeated firing over specified period of time)
  - environmental testing (for extreme temperatures/humidity; sand/dust/mud/immersion in salt water)
  - drop test (gun and ammunition clip, loaded and unloaded)
  - chemical compatibility with nonmetallic materials (various cleaners/solvents/oils/fuels/lubricants/decontaminants/water)
  - specialized test firing (with gloves, wet/dry; cold/muddy/bloody hand or gun)
  - electromagnetic immunity, emissions, jamming and intentional bypassing

Battery

- On a battery-operated weapon, indicator shows if power is low.

Training and Enrollment

- Minimal new training required.
- Additional users can be added and/or ownership transferred.
- Weapon able to recover from damaged or lost authenticator.

Assembly and Disassembly

- Weapon can be repeatedly disassembled and reassembled for cleaning, maintenance, and training as for conventional gun.

---

[a] The false reject rate (FRR) is a measure of the likelihood that a security system will incorrectly deny access to an authorized user. It is typically stated as the ratio of the number of false rejections divided by the number of identification attempts.

[b] The false acceptance rate (FAR) is a measure of the likelihood that a security system will incorrectly grant access to an unauthorized user. It is typically stated as the ratio of the number of false acceptances divided by the number of identification attempts.

[c] If there are children in the home, the UAHG can fail in the unarmed or inactive mode. If the gun owner does not anticipate accidental use by a child, it can fail in the armed or active mode.

[d] Traditional authorization schemes assume that authorization means enabling, or activating, the technology in question. However, authorization might also mean disabling, or deactivating, a technology. In the case of a handgun, an operable handgun could be disabled through a voice command from an authorized user. This scheme could operate alone, or it could be paired with a more traditional scheme, in which the user activates the handgun through contact with a biometric sensor on the firearm and deactivates it through a voice command.

Authentication[3]

People are authenticated so that their requests to do something—in this instance, fire a handgun—can be authorized. Authentication factors are usually grouped into three categories: (1) what you know (e.g., password, passphrases, PINs); (2) what you have (e.g., security token, bank card, key); and (3) who you are (e.g., biometric).

The category of "what you know" is characterized by secrecy or obscurity. This includes memorized passwords and "obscure" information, which can be loosely defined as "unknown to most people." Your mother's maiden name and your favorite color are examples of this type of information. A security drawback of secrets is that, each time they are shared for authentication, they become less secret.

The category of "what you have" is characterized by physical possession. For instance, house keys are tokens that have stood the test of time. A security drawback of a house key is that, if it is lost or stolen, the person who now has it will be able to enter the house. This is why many digital tokens are combined with another factor, such as an associated password or PIN. One advantage of a physical object used as an authenticator is that, if it is lost, the owner becomes aware of this and can act accordingly.

The category of "who you are" is characterized by its distinctiveness to one person. A biometric is a measure of a physical characteristic of a person and includes such things as fingerprints, eye scans, voiceprints, and signatures. Even though a biometric may not have "one-in-the-world" uniqueness, a good biometric is distinctive enough so that two biometric authenticators will rarely be exactly alike, at least within the scope of a particular implementation. An advantage of a good biometric is the difficulty to copy (or spoof) it. A disadvantage of most biometrics is that, if they are compromised or stolen, they cannot be changed as easily as memorized passwords or physical tokens.

Biometric Authentication

Biometric authentication is based on a unique physical characteristic of the authorized gun user (who you are). The state of the art in biometrics

---

[3] For more information about authentication, the interested reader may wish to consult the two Sandia reports (1996, 2001), the NJIT report (2001), and O'Gorman (2003).

is such that it is very difficult to reliably match a single person against a database containing a large number of biometrics (i.e., one-to-many matching). Therefore, one-to-one verification or one-to-few matching is usually the preferred approach when the match is done exclusively by machine, as would be the case in the UAHG application. Biometrics for UAHG authorization may include the following characteristics:

- eye characteristics[4] (e.g., retina, iris)
- voice recognition
- hand characteristics (e.g., fingerprint,[5] palm print, finger length/hand geometry, skin texture, grip pressure,[6] subcutaneous/spectroscopic skin features[7])
- other characteristics (e.g., face recognition, handwritten signature, keystroke signature, gait, thermal signature)

Based on the experience embodied in several of the committee members, the committee believes that only five biometric technologies can fit and function on a handgun and meet the requirements and specifications outlined in Table 3: fingerprint, voice recognition, skin texture, skin spectroscopy, and handgrip pressure.

Token-Based Authentication

There are a variety of token-based, or object-based, authentication technologies, but at this time the committee is aware of only one, based on radio-frequency identification (RFID), that is under development for application to UAHGs. An RFID system generally consists of a reader and transponder that is associated with an entity to be identified. Transponders, also called RFID tags, may be attached to, embedded in, or in the proximity of the entity to be identified. Readers send requests for identity information to one or more tags using a radio frequency that is compatible with the tags of interest. Tags respond with the requested information,

[4]Presently used in facility-access systems.

[5]Was investigated by S&W for a UAHG but has since been abandoned.

[6]Advocated by NJIT for UAHG in basic/applied research phase.

[7]Presently being developed by S&W.

either by transmitting a signal using the energy received from the signal sent by the reader (passive RFID) or by generating a signal, which may include additional, environment-specific information, using their own batteries (active RFID).

If the reader receives the correct response, it activates either an electronic firing mechanism coupled to the trigger or actuates a mechanism that removes a safety lock or mechanical obstruction of the firing pin. The information in the transponder's reply typically includes ID information. One of the main advantages of this method of identification is that it works well under most adverse environmental conditions (with the exception of RF interference near the system's operating frequency).

A variety of RFID systems have been designed for a variety of purposes. Tags can be read only, read-write, and write-once-read-many times. They may or may not include security protocols to protect the confidentiality and/or the integrity of the information. RFID systems operate at a variety of frequencies and power levels. They have become very popular over the past 10 or 15 years as the result of new, low-cost implementations, the development of RFID standards, and the emergence of efficient information-technology systems that can collect and apply the information collected from tags.

The main advantage of passive RFID systems is that the tags do not require batteries; thus, they have a very long shelf life. Passive RFID systems are used for electronic product code (EPC) technology. Because so many of RFID tags are produced each year, they are very inexpensive. EPC tags, for example, cost about 30 cents or so today, and the price may drop by an order of magnitude if anticipated volumes are produced. The manufacturing costs of passive RFID tags for UAHGs could also be very low (less than a dollar). The cost of the reader would be determined by the cost of the battery and the cost of building the reader into the handgun.

If an RFID transmits a static ID code, such as the codes used for EPCs, it could be easily spoofed. Therefore, an RFID tag for a UAHG would have to hold more than an ID number. This problem has been addressed in at least one other application, in which the tag responds in a unique way every time it is read (Box 3).

In a UAHG system, the tag would either be worn by or embedded in the user. An embedded tag would become a "virtual biometric" because it would be permanently or semi-permanently associated with an individual, which would avoid the problem of loss or theft of the key. The embedded

BOX 3
RFID Tags for Vehicle Immobilization

A number of different RFID systems are used for vehicle-entry control and immobilization. For vehicle immobilization, the tag is typically embedded into an ignition key, and the reader is embedded in the key receptacle. The tag and reader may have a common symmetric key, or the reader may contain the public part of a public/private key pair, while the tag contains the private part. When the ignition key is mechanically engaged, the reader sends a challenge to the tag, via RF. The challenge includes a random value that is used only that time. When the tag receives the random value, it uses the symmetric or private key to perform a computation with the random value and returns the result to the reader. If the expected result is returned, the electronic ignition is actuated.

At least one of these systems has reportedly been broken by a "white-hat" security team at Johns Hopkins University (Roberts, 2005). However, the attack could have been thwarted if the system cryptography had been more robust.

tag would be similar enough to a true biometric that the committee believes it should be considered as a potential technology for UAHGs.

FN Manufacturing has proposed using such a system (Verichip) in its UAHG (Applied Digital Solutions, 2004). The RFID Verichip system is a passive tag technology, and the tag can be injected into the human body. When an individual with an embedded tag passes near a reader, the tag transmits a unique user code. The code is then securely transmitted from the reader to a database from which the user's medical information, payment authorization, or other information can be retrieved. In the case of a UAHG, the database would contain the public "keys" of authorized users and might be housed within the handgun itself.

A tag embedded under the skin may raise health and other concerns. The Food and Drug Administration's notification letter approving the Verichip system noted a number of potential health risks (e.g., adverse tissue reaction, migration of the implanted transponder) and other risks (e.g., compromised information security, failure of the implanted transponder, failure of the inserter, failure of the scanner, electromagnetic interference, electrical hazards, and magnetic resonance imaging incompatibility). A

number of groups, such as the American Civil Liberties Union (Steinhardt, 2004), have suggested the use of RFID tags raises privacy issues.

Latching and Firing Mechanisms

In order for a user to be authorized, the authentication system must interface with a component on board the gun. Presently, handguns and most rifles have mechanical latching mechanisms that cock and release the hammer or striker, which drives the firing pin into the primer. The authentication electronics must, therefore, interface with the mechanical latching mechanism. An alternative to mechanical latching is an all-electronic firing mechanism (no firing pin) that "detonates" the cartridge. Some gun manufacturers believe that all-electronic firing mechanisms will be more reliable for a UAHG than mechanical methods because they will eliminate the need for an electromechanical interface. FN Manufacturing is developing a weapon with a mechanical latch, but the S&W and NJIT project teams are developing all-electronic handguns.

External mechanical locks (e.g., trigger locks) are devices that prevent the gun from firing. They are most useful in situations in which the gun user is not under stress or time pressure during the locking and unlocking procedure. Safety in the home can be greatly improved if the gun owner keeps the gun "locked." However, because external mechanical locks are not suitable for the scenarios examined in this study, they will not be considered further.

Enrollment

Any UAHG system must have a method for enrolling authorized users. As noted in the first Sandia report (SNL, 1996), enrollment could be done either by software and hardware in the handgun or by a device separate from the weapon. In the latter case, there would need to be an interface between the enrollment device and the handgun and, possibly, a permanent or semi-permanent database to store the identifying information of authorized users. Enrollment may raise security and privacy risks, particularly if there is an interface that connects the UAHG to a remote server over the Internet (NRC, 2003).

Enrollment schemes often use an administrator who has the authority to activate the enrollment process for new authorized individuals. For example, in the case of handgrip authentication, the administrator might grip

and release the firearm several times in quick succession to switch the gun to the enrollment mode. If enrollment were done on a device separate from the firearm, an administrator would still be needed to activate the process, and the new enrollment information would have to be transferred to the handgun.

Enrollment for a UAHG using a non-biometric authentication technology such as RFID could occur much the same way as for a biometrics-based system. The administrator would need to switch the transponder in the handgun to enrollment status, perhaps by depressing a button on the weapon. The gun would then challenge the enrollee's tag with a special code, and the enrollee tag would respond with its public key and an error-detecting code. The gun would challenge the tag again using the normal challenge to be used to enable the gun, and the enrollee tag would respond as it normally would, using the private key, to confirm the enrollment.

It should also be possible to enroll multiple new users at one time, as might be desired in a law enforcement application, where several officers require access to the same firearm. For such bulk enrollment, the handgun would need to carry out a dialog with a computer. In the case of RFID, the computer would load a sequence of public keys known to be the keys used in the tags held by the appropriate enrollees; in the case of biometric-based authentication, the unique biometric templates would be loaded. Whatever the authentication technology, there also must be a process for de-enrolling authorized users. And if the administrator is no longer able to provide enrollment access, a "super administrator" hierarchy that includes an armorer (in the case of law enforcement), firearms dealer, or firearms manufacturer can be established.

The design of an enrollment system will need to consider various failure possibilities. For instance, how is enrollment to be done—and who should do it—if the authenticator (e.g., an embedded RFID tag) is damaged? If the enrollment process itself fails, perhaps due to a software glitch, is there a workaround or back-door approach for enrolling a new user? Who would do that? Enrollment might also have to account for non-technical factors that could affect authorization. For example, to prevent criminal access to a UAHG, the enrollment process might need to be tied to a database of convicted felons.

Those working to develop a UAHG at this time appear to be focusing their resources on solving the design challenges associated with the handgun itself. Ultimately, a UAHG will have to incorporate enrollment technology, and this will have cost and time-to-market implications.

OBJECTIVE 4: TECHNOLOGY-READINESS ASSESSMENT

The list of applicable authentication technologies has not changed substantially since the original Sandia report was published in 1996. Some implementations of the technologies have progressed, although primarily in non-gun-related applications. For example, RFID tags are being used for logistics tracking and control and automatic toll collection, and both RFID and biometrics are used for building-access control. Mechanical latching remains a critical component of the design of a UAHG with a mechanical firing mechanism. A newer entrant to the technology mix is an electronic firing system, which eliminates the electromechanical interface but requires specialized ammunition. And finally, of course, all of the electronic components that service the authorization reader, drive a mechanical latch mechanism, or enable electronic firing must be miniaturized and fitted into the configuration of the gun. These technologies constitute the main building blocks of a UAHG.

The committee's estimates of technology readiness are based on publicly available information from the NIJ projects, the state of the art of the underlying technologies, such as authentication schemes, and the expertise of committee members in R&D and manufacturing in general and in the manufacturing and testing of guns in particular.

Biometrics

Law-Enforcement Use

Table 4 suggests the suitability of biometric and RFID authentication technologies for integration into a UAHG for law-enforcement use, where the primary concern is loss of a gun in a struggle. These ratings are suggested by members of the committee based on their expertise and prior experience. They range from 1 for the least likely to 5 for the most likely candidate. A rating of 1 means the technology is not likely to ever meet the specification; 2 means the technology in its current form does not meet the specification and may be less than optimal even with further R&D; 3 means the technology in its current form does not meet the specification or meets it incompletely, but it may be more suitable with further R&D; 4 means the technology meets the specification but could be improved; 5 means the technology meets or exceeds the specification and needs little or no improvement. For some newer biometrics about which less is known, an educated guess is indicated by parentheses.

TABLE 4 Suitability of Biometrics and Embedded RFIDs for Law-Enforcement Use

	Fingerprint	Voice	Skin Texture	Skin Spectroscopy	Handgrip	RFID Reader	Embedded RFID Tag[a]
Size and weight	4	4	(4)[e]	(4)	(4)	4	5
Speed	4	2	(4)	(4)	(3)	4	5
Power	3	3	(3)	(3)	(3)	4	5
FRR[b]	2	1	(2)	(2)	(2)	4	4
FAR[c]	4	4	(3)	(3)	(3)	4	4
Durability	4	4	(4)	(4)	(4)	4	4
Temperature	3	5	(3)	(3)	(4)	4	5
Dirt and noise	1	1	1	1	(3)	4	5
Ergonomics	3	n/a	3	3	(4)	4	4
Glove[d]	1,4	4	1,4	1,4	3	5	5
Cost	3	3	(2)	(2)	(2)	3	5

[a]The ratings for RFID tags assume that the reader is integrated into the gun, is powered by a battery similar to the way batteries are used for circuitry in biometric readers, and that there is a redundant switch on the gun. The RFID reader is powered when, and only when, the gun is grasped. When the gun is not in use, no current is drained from the battery.

[b]FRR = false rejection rate.

[c]FAR = false acceptance rate.

[d]Two numbers are listed when a glove is worn. Most of the biometrics cannot be read through a glove (the first number). However, it is conceivable that an officer's glove might have a window, or hole, at the position of the sensor for use with a UAHG (second number).

[e]Numbers in parentheses indicate educated guesses based on limited data.

The authentication mechanism for law-enforcement users could either enable the gun or enable *and* disable the gun. For a biometric that operates when a hand is in contact with the gun, the biometric is read continuously or nearly continuously; the gun is enabled when held by the officer and disabled when not held by the officer. A voice biometric would require that the officer vocalize a command to enable the gun and vocalize a separate command to disable the gun. The gun could be left in either mode indefinitely. If any authentication mechanism fails due to loss of power, the gun must be enabled.

A low FRR (false rejection rate) is very important for law enforcement because it ensures that authorized officers will not be rejected. The FAR (false acceptance rate) is not as important because, if a gun is wrested away in a confrontation, an adversary is not likely to have either the time or the composure to repeatedly engage the authentication system in the hopes of being wrongly authorized.

Homeowner Use

Many of the requirements for law enforcement, such as operability in extreme temperatures and other adverse environmental conditions, durability, and operability with glove use, are not as important for homeowners' weapons, as the committee has defined them. The FAR, however, is very important for homeowners because there must be a very low probability that an unauthorized person (e.g., a child) will be falsely authorized. Spoofing, the process of "deceiving" an authorizing system so that it incorrectly allows access to an unauthorized person, is also a great concern to homeowners. Some fingerprint readers, for example, can be spoofed by fingerprint images imprinted on pieces of jellied candy. Thus, antispoofing to prevent an unauthorized child or teenager who might lift the fingerprint of a parent and create a spoof fingerprint from using a gun is required for a UAHG. The suitability of biometric and RFID technologies for integration into a UAHG for homeowner use is shown in Table 5.

Appropriate Biometrics

Considerable work is being done on fingerprint and iris sensing as a component of access-control systems and on voice recognition for computer-automated querying systems. As more robust sensors and recognition algorithms are developed, these biometrics might eventually be

TABLE 5 Suitability of Biometrics and Embedded RFID for Homeowner Use

	Fingerprint	Voice	Skin Texture	Skin Spectroscopy	Handgrip	RFID Reader	Embedded RFID Tag
Size and weight	4	4	(4)[a]	(4)	(4)	4	5
Speed	4	2	(4)	(4)	(3)	4	5
Power	3	3	(3)	(3)	(3)	4	5
FRR	3	2	(2)	(2)	(2)	4	4
FAR	4	4	(3)	(3)	(3)	4	4
Anti-spoof	3	3	(2)	(2)	(3)	4	5
Ergonomics	3	n/a	3	3	(4)	4	4

[a]Numbers in parentheses indicate educated guesses based on limited data.

useful for a UAHG. However, at present, the committee is aware of only two true biometrics (skin spectroscopy [by S&W] and handgrip pressure [by NJIT]) that are being adapted for handguns, and neither has reached the level of discrimination required by law enforcement specifications.

S&W and NJIT believe they will achieve the required levels of discrimination for skin spectroscopy and handgrip-pressure technology, respectively, but it is a rule of thumb in the biometrics community that data on the sensitivity and reliability of a sensor technology are not considered valid unless or until they have been confirmed by unbiased third-party testing. Both implementations are at a breadboard stage—the sensor is in a realistic configuration in the gun, but the electronics for the reader are external to the gun. Although the miniaturization of electronics is relatively straightforward, the design and manufacturing iterations of the electronics could be costly, and achieving the necessary form factor could be difficult. Lacking a full-up brass-board model, third-party data on discrimination, and convincing identification of users wearing gloves, the committee concludes that both technologies are at a TRL 4,[8] at best.

The other biometric technologies, which are not being investigated for a gun application, are at TRL 3[9] or lower. S&W abandoned its investigation of fingerprint technology in the late 1990s after concluding that reliable readings could not be obtained with available technology. (Fingerprint recognition technology has improved since then.) FN Manufacturing concluded that handgrip-pressure technology was unreliable, although NJIT claims that its implementation of this approach will work.

Radio Frequency Identification

In the technology evaluation in the 1996 Sandia report, RFID tags, which scored the highest, are apparently the only "what-you-have" authorization technology presently used in a gun application. iGun, a subsidiary of

[8]TRL 4: Component and/or breadboard validation in laboratory environment. Basic technological components are integrated to establish that the pieces will work together, but the system is "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in a laboratory.

[9]TRL 3: Analytical and experimental critical function and/or characteristic proof of concept. Active R&D is underway, including analytical studies and laboratory studies to validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.

Mossberg, markets a shotgun with an RFID-authorization system that requires the user to wear a ring that communicates with a transceiver in the gun. Compared with a standard handgun, the larger shotgun, especially the larger stock, provides ample room for on-board electronics and batteries. The iGun website (*www.iguntech.com*) notes that if the shotgun is exposed to "severe situations, if it gets submerged, thoroughly soaked, or shocked from an unusual drop or impact, it should be returned to the factory immediately." This suggests the system is not robust enough for either handgun application considered in this study. Metal Storm, which is a partner with NJIT in the development of a handgun with handgrip-pattern-recognition technology, has also advocated a system that would require an authorized user to wear a ring with an RFID tag (Metal Storm, 2003).

Barriers to implementing an RFID-authorized UAHG are: possible RF interference; possible reader interference caused by two tags in close proximity; too large or small a reading range (for law enforcement, a reader must not be able to "see" the tag on an officer whose handgun is picked up by an adversary some distance away or limited to detect a tag only at very close range). A significant drawback of RFID technology is that a ring, bracelet, or other accessory worn outside the body containing the tag can be lost or stolen, either rendering the gun unusable by anyone or allowing an unauthorized person, such as a child, to operate it In fact, handgun developers and potential law enforcement users consider this problem insurmountable. Metal Storm's comments not withstanding, all efforts to use "external" RFID tags to develop a UHAG have been abandoned.

One can imagine that law enforcement officers might be willing to have a "chip," a virtual biometric RFID tag, inserted as a reasonable requirement of the profession. Homeowners, however, may be much less willing to carry an embedded tag, both because of possible health concerns and because of potential privacy issues. But this is primarily a social-acceptability issue, not a technology issue. iGun (2004), which received funding from NIJ to evaluate the potential of various biometric technologies, reached a similar conclusion about the technical merits of implantable RFID chips. In terms of the technology, anyone who has used an RFID building-access system understands that the sensor recognizes authorized entrants in a fraction of a second and appears to the casual observer to have zero FAR and FRR. In short, the technology works quite well.

Considering that RFID technology in general is mature and that the development of embedded RFID sensor technology is being driven by

medical applications and has been approved by the FDA, the committee rates the embedded sensor technology at TRL 7[10] or TRL 8.[11] However, these RFID authorization systems do not require miniaturized readers. Thus, considerable technology development may still be necessary to fit the reader electronics into the gun. FN Manufacturing has been very circumspect in releasing public information, so it is not clear how much progress has been made toward integrating the RFID reader into a brassboard gun. Nevertheless, because the reader technology should work at the breadboard stage, the committee rates it at TRL 5.[12]

Latching Mechanisms

Gun companies may be expected to have competence and experience in developing the mechanical enable and/or disable mechanism of a gun. However, this is not an easy task. Reliable handguns require precision manufacturing, and they are very compact, which means they have limited clearances for the addition of new mechanical or electromechanical systems.

Once again, different developers have taken different approaches to the problem. S&W believes that the electromechanical latching system may compromise reliability and has therefore chosen to develop an all-electronic weapon. FN Manufacturing has chosen to take the mechanical-latch approach. The committee believes that, although an electromechnical latch may not be the most elegant solution, it could be brought to TRL 6 in relatively short order.

---

[10]TRL 7: System prototype demonstration in an operational environment. Prototype near or at planned operational system level. Represents a major step up from TRL 6, requiring the demonstration of an actual system prototype in an operational environment, such as in an aircraft, a vehicle, or space. Examples include testing the prototype in a test bed aircraft.

[11]TRL 8: Actual system completed and "flight qualified" through testing and demonstration. Technology has been proven to work in its final form and under expected conditions. In most cases, TRL 8 represents the last level of system development. Examples include developmental testing and evaluation of the system in its intended weapon to determine if it meets design specifications.

[12]TRL 5: Component and/or breadboard validation in a relevant environment. Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.

Electronic Firing Systems

The vast majority of guns are fired by the forceful mechanical striking of a primer with a firing pin. However, a properly designed primer can also be ignited with an electrical charge. One simply exchanges mechanical components for a power source. For "regular" guns, that is, not UAHGs, one can debate which system is more reliable and cost effective. Certainly, gun manufacturers prefer mechanical guns. However, the added complexity of an electromechanical locking/unlocking scheme for UAHGs may justify an electronic firing system. Both S&W and NJIT appear to have reached this conclusion.

Until very recently, Remington offerred an electronically fired rifle using its own 22-250 and 220 Swift Etronix ammunition. The electronic handgun developed by S&W used the primer from that ammunition and had a conventional magazine. S&W has reported firing 60,000 rounds with prototype electonic weapons with no problems in firing reliability or power-source limitations. S&W indicated that the firing electronics were fully integrated into the gun (Kevin Foley, S&W, personal communication, 4/20/05). Given the experiences of Remington and S&W, the committee judges that the S&W electronic firing mechanism is at least at TRL 6,[13] and possibly at TRL 7.

NJIT has reported that its handgrip-pressure technology will be interfaced with an electronically fired handgun made by Metal Storm. The design of the Metal Storm gun is radically different from the design of the S&W and Remington electronic guns. In the Metal Storm gun, the projectiles are stacked in the barrel and fired in sequence. Thus, in principle, the gun could have multiple barrels and fire rounds in very rapid succession for extreme firepower. Metal Storm (2003) has built at least two seven-shot "demonstrator" handguns, but the company has provided few details about their reliability. Recently, Metal Storm announced that the timetable for producing a commercial handgun using its technology has been extended because NJIT's grip-sensor technology was not ready to be integrated with

[13]TRL 6: System/subsystem model or prototype demonstrated in a relevant environment. Representative model or prototype system, which is well beyond the breadboard system tested for TRL 5, is tested in a relevant environment (sometimes referred to as a brassboard model). Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high fidelity laboratory environment or in simulated operational environment.

the Metal Storm technology (LHA, 2005). Because this is a rather new concept and even the ammunition will require development, the committee concludes that this technology is at at TRL 3, 4, or 5.

The failure mode of a UAHG is a critical issue. With an electromechanical latching system, if the power to drive the latch fails, the gun could be armed, as is necessary for law enforcement, or unarmed, as appropriate for homeowners. If the gun is stolen, the design should be such that removing the latching mechanism will disable the gun.

If the power to fire the primer in an electronic gun were lost, the gun would be unarmed, and careful maintanence would be necessary to be certain that power would be available to the primer. If an electronic gun were stolen, efforts to strip the electronics would probably render the gun useless. Replacing or modifying the existing electronics to allow unauthorized access, although technically possible, would be expensive and would be well beyond the abilities of most people.

An additional issue (not related to TRL), is that the primer for available electronically fired ammunition is about five times as expensive ($75 for 1,000 rounds) as conventional primer, which results in about a 10-percent premium over conventional rounds. This could have a negative impact on the overall market for electronically fired guns, especially on potential high-volume users of the new primers, such as mid- to large-size police departments, and on sport shooters, who might otherwise have been early adopters because of their interest in novel technologies.

Systems Integration

Based on the information available, the committee believes that progress on technology integration has been minimal. S&W appears to have successfully integrated the electronic-firing and biometric sensor components, but the electronics for the reader are external to the gun. FN Manufacturing, with support from NIJ, has put a great deal of effort into interviewing law enforcement officers to establish detailed requirements and specifications for a UAHG. The list includes "must haves" as well as "nice to haves." FN is not required to produce a model until the last phase of the NIJ-supported project, so the extent of its systems integration is not known. NJIT, which has been focused on developing handgrip-pressure authorization technology, and Metal Storm, which is working on novel gun technology, may not have begun working on the integration of these technologies into a weapon.

Cost Considerations

The committee estimates that a moderate design change in a conventional gun would take approximately three years and cost somewhere between $3 million and $4 million (see Appendix D, developed by the committee, for a breakdown of estimated costs). Development costs would be increased by several hundred thousand dollars if electronic ammunition had to be used in testing.

The extensive experience of gun companies in the development of gun technologies has kept the costs of conventional guns fairly low. However, the development of a UAHG will require technologies that are beyond the traditional experience base of gun companies. Through the NIJ program, S&W, FN Manufacturing, and NJIT have already spent or will soon spend amounts on UAHG development approaching the development costs of a conventional gun. Nevertheless, in the committee's judgment of TRLs, no one is close to having integrated brass-board test articles (present systems are at a level of TRL 5 or less). There is little evidence that these groups have begun serious development of enrollment-system technology.

Furthermore, these are early-stage costs. Typically, absent an experience base, development costs escalate rapidly from this point forward. The costs will include further development of component technologies, systems integration, extensive testing and evaluation of prototypes, and development of new production tools—all compounded by potential liability issues. Thus, based on the experience of members of the committee in product development, the committee estimates that total costs to bring a single implementation of a UAHG to market could easily reach several times to as much as 10 times what each developer has spent to date, or on the order of $30 million, particularly for a version that uses true biometric authentication. Timing would depend on the rate of investment, but, given the investment capacity of gun companies, it could take 5 to 10 years to reach full production.

Compared to the development costs for some products, these costs are still fairly modest. However, as summarized in the NJIT report, the gun industry as a whole is highly leveraged and has minimal capacity for, and a minimal track record of, speculative R&D. It seems to the committee that the development of a UAHG is, indeed, a speculative enterprise because there is no indication, or at least no way to verify, that a significant market will exist for such a gun if it is successfully developed. If the development of a UAHG costs 5 to 10 times as much as the development of a conventional

firearm, the developer must either defray those costs over a considerably larger market (which, from the point of view of the gun company, could cannibalize the conventional gun market) or charge a premium price. It is conventional wisdom that a UAHG will not sell if its cost exceeds that of a conventional gun by more than $100 or so. Considering that the additional technology components could easily account for most of that differential, there will be little room for a profit margin.

Given the history of R&D in the gun industry and the speculative market prospects for a UAHG, the committee concludes that the NIJ program has been a prime driver of UAHG technology development; thus, NIJ is responsible for much of the real progress, as opposed to concept development, that has been made to date. However, because the fiscal 2005 NIJ budget does not include follow-on funding for UAHG development, it would not be surprising if existing development efforts come to a halt. As a case in point, Colt did not share in the 2000–2004 NIJ program and discontinued its UAHG development.

FINDINGS

A UAHG for law enforcement presents some very challenging problems. Requirements include a very low FRR and a weapon that can function reliably in adverse environmental conditions, high-stress situations, the presence of dirt, and with users wearing gloves. In addition, both the skin-spectroscopy and handgrip-pressure technologies under development remain unproven, high-risk technologies in terms of the likelihood of successful development.

A UAHG for homeowners has less stringent authorization requirements, although no on-gun solution can satisfy all of the requirements today. Inclement weather, dirt, and gloves are not significant factors, assuming the gun remains in the home, but the weapon must recognize an authorized user in a stressful situation, and the gun should share the requirement of a law enforcement gun of being extremely difficult for an unauthorized person intentionally to bypass the security system. However, if the emphasis is on the rejection of an unauthorized user, especially a child, the demands on the sensor are likely to be somewhat less stringent. Thus, in designing a UAHG for homeowners, the product designer must choose between a "perfect"' solution and a "good" solution.

Unlike the biometric technologies being considered, RFID sensing appears to be a relatively low-risk technology that has an extensive, well

documented track record in other applications. Like biometric sensors, however, it will require miniaturized components to be integrated into the gun. Although miniaturization will not be a trivial or low-cost undertaking, the committee believes it is doable. The primary drawback of RFID authorization in the past was that it was a "what you have" technology (e.g., a key), which was susceptible to loss. However, with the availability of a tag that can be inserted under the skin of the wrist or hand, RFID authorization becomes a "who you are" technology, like a biometric. User acceptance is an issue, of course, but this appears to be an elegant technical solution.

A UAHG can be built with a mechanical or an electronic firing system. Integrating a mechanical latching mechanism into the close confines of a handgun is a demanding task, but gun manufacturers have a great deal of experience in mechanical design. With mechanical latching, the fail-safe mode of a gun can be armed (for law enforcement) or unarmed (as an option for homeowners). Electronic firing of a handgun (60,000 rounds with good success) has been demonstrated by S&W. If the authentication technology in an electronic gun stops working, the gun can also fail unarmed or armed, unless it loses all power, in which case it can only fail unarmed.

Although a good deal of progress has been made since the concepts for a UAHG were identified in the 1996 report from Sandia National Laboratories, development has not progressed to the point of producing an integrated brass-board model. Thus all of the concepts still have TRLs of 5 or lower. If efforts to create a UAHG were to be started over using present developments as the baseline, the committee believes that the shortest path to introduction of a commercial UAHG would involve development of a mechanical or electronic gun interfaced with an RFID tag inserted under the skin. Biometric technologies simply have too much uncertainty.

The NIJ program has provided several million dollars each to S&W, FN Manufacturing, and NJIT for early-stage technology development. Typically, development costs escalate rapidly as multiple design models are created. The committee estimates it could cost several times to as much as 10 times as much as the redesign of a conventional handgun (about $30 million) and take 5 to 10 years to bring a UAHG to market. The development costs of an embedded RFID with an electromechanical or electronic UAHG system might be near the low end of the cost and time ranges. The development of a true biometric UAHG system would more likely be near the high end.

Recent progress in the development of a UAHG has been almost solely

due to the NIJ program. However, no follow-on funding has been included in the 2005 fiscal year federal budget for this program. The committee is not aware of any substantive developments outside the NIJ program and, therefore, expects that present development efforts will come to an end when NIJ funding runs out.

It is not known what fraction of law-enforcement officers or homeowners would be interested in paying a higher price for a UAHG and accepting the trade-offs that would come with more complicated technology (e.g., the risk that the gun would fail to fire for an authorized person). The Sandia reports of 1996 and 2001 indicated that law enforcement officers at that time were skeptical of the technology, at best. In addition, the number of "takeaway deaths," the problem a UAHG was intended to address, has decreased to single digits in all but one of the last 13 years for which data are available. Law enforcement might conclude, therefore, that the technology risk is greater than the risk of a takeaway and that they now have less incentive to champion the development of a UAHG or to pay a premium to acquire such a gun. That attitude could change if the weapons were demonstrated to be highly reliable.

The number of handgun-related deaths and injuries in the population at large, however, particularly among children who accidentally discharge a loaded weapon and people attempting suicide, suggests that there is a significant danger associated with unsecured handguns in the home. Considering the size of the market for child-safety products, cost may not be as significant an issue in this market.

REFERENCES

Applied Digital Solutions. 2004. Verichip Corporation enters into a memorandum of understanding for the development of a firearm's user authorization system—"Smart Gun"—using Verichip RFID technology. Press release. Available online at: *http://www.adsx.com/news/2004/041304.html* (February 13, 2005).

BATF (Bureau of Alcohol, Tobacco, Firearms, and Explosives). 2005. Annual Firearms Manufacturing and Export Report—2003. Available online at: *http://www.atf.treas.gov/firearms/stats/afmer/afmer2003.pdf.* (May 23, 2005).

BJS (Bureau of Justice Statistics). 1995. Firearms, Crime, and Criminal Justice: Guns Used in Crime, by W. Zawitz. Selected Findings. July 1995 NCJ-148201. Available online at: *http://www.ojp.usdoj.gov/bjs/pub/pdf/guic.pdf* (April 27, 2001).

BJS. 2004. National Crime Victimization Survey, Criminal Victimizations, 2003. Available online at: *http://www.ojp.usdoj.gov/bjs/pub/pdf/cv03.pdf* (February 9, 2005).

Brady Center to Prevent Gun Violence. 2001. Targeting Safety: How State Attorneys General Can Act Now to Save Lives. Available online at: *http://www.bradycenter.org/xshare/pdf/reports/targetingsafety.pdf* (February 10, 2005).

Cook, P.J., B.A. Lawrence, J. Ludwig, and T.R. Miller. 1999. Medical costs of gunshot injuries in the United States. Journal of the American Medical Association 282: 447–454.

FBI (Federal Bureau of Investigation). 2003. Law Enforcement Officers Killed and Assaulted—2003. Available online at: *http://www.fbi.gov/ucr/killed/leoka03.pdf* (February 9, 2005).

GAO (General Accounting Office). 1999. Best Practices: Better Management of Technology Development Can Improve Weapon System Outcomes, edited by L. Rodrigues and P. Francis. GAO/NSIAD-99-162, July 1999. Washington, D.C.: General Accounting Office. Available online at: *http:/www.gao.gov/archive/1999/ns991620.pdf*.

iGun Technology Corp. 2003. The Use of Biometrics to Control Access to a Personalized Law Enforcement Handgun. Final report for work completed under contract from the National Institute of Justice. Available online at: *http://www.igun.com*.

LHA (Lippert Heilshorn & Associates). 2005. Metal Storm revises handgun development timetables. Press release dated Jan. 31, 2005. Available online at: *http://www.lhai.com/docs/31%20Jan%20Handgun%20release.doc* (February 13, 2005).

Metal Storm, Inc. 2003. Advanced Smart Gun System for Law Enforcement Applications. Unpublished final report for work completed under contract from the National Institute of Justice. June 2003.

NAE (National Academy of Engineering). 2003. Owner-Authorized Handguns: A Workshop Summary, edited by L.A. Davis and G. Pearson. Washington, D.C.: National Academies Press.

NIJ (National Institute of Justice). 1993. Gun acquisition and possession in selected juvenile samples, edited by J.F. Sheley and J.D. Wright. Research in Brief, NCJ-145326. Washington, D.C.: National Institute of Justice and Office of Juvenile Justice and Delinquency Prevention.

NJIT (New Jersey Institute of Technology). 2001. Personalized Weapons Technology Project: Progress Report with Findings and Recommendations, Vols. 1 and 2. April 15, 2001. Newark, N.J.: New Jersey Institute of Technology.

NJIT. 2003. New Jersey Institute of Technology moves ahead to get smart gun on market. Press release, September 5, 2003. Available online at: *http://www.njit.edu/v2/News/Releases/395.html* (April 20, 2005).

NRC (National Research Council). 2003. Who Goes There?: Authentication Through the Lens of Privacy. Washington, D.C.: National Academies Press.

NRC. 2005. Firearms and Violence—A Critical Review, edited by C.F. Wellford, J.V. Pepper, and C.V. Petrie. Washington, D.C.: National Academies Press.

O'Gorman, L. 2003. Comparing passwords, tokens and biometrics for user authentication. Proceedings of the IEEE 91(12): 2019–2040.

Roberts, P. 2005. RFID crack raises spectre of weak encryption. PC World, March 18, 2005. Available online at: *http://www.pcworld.idg.com.au/index.php/id;102583488;fp;512;fpid* (April 22, 2005).

SNL (Sandia National Laboratories). 1996. Smart Gun Technology Project Final Report, edited by D.R. Weiss. SAND-96-1131 Available from National Technical Information Service, Springfield, Va. NTIS Order Number: DE96013854.

SNL. 2001. Smart Gun Technology Update, edited by J.W. Wirsbinski. SAND-2001-3499. Available from National Technical Information Service, Springfield, Va. NTIS Order Number: DE2001-789587.

Steinhardt, B. 2004. Statement of Barry Steinhardt, Director of the ACLU Technology and Liberty Program, on RFID tags before the Commerce, Trade and Consumer Protection Subcommittee of the House Committee on Energy and Commerce. July 14, 2004. Available online at: *http://www.aclu.org/Privacy/Privacy.cfm?ID=16104&c=130* (April 25, 2005).

Tartaro, J.P. 2005. Taurus withdraws from 'smart gun' partnership in NJ. Kansas Sportsmen's Alliance. Available online at: *http://www.theksa.com/News.htm#36*. (March 17, 2005)

TIM (Taurus International Manufacturing). 2003. Authorized user firearm partnership. Press release dated November 25, 2003. Miami, Fla.: Taurus International Manufacturing.

Violence Policy Center. 2002. Firearms Production in America 2002 Edition. Appendix Four—Domestic Production of Civilian Firearms, 1899 to 2000 (In Thousands). Available online at: *http://www.vpc.org/graphics/prod2002.pdf* (February 9, 2005).

Vyrostek, S.B, J.L. Annest, and G.W. Ryan. 2004. Surveillance for fatal and nonfatal injuries—United States, 2001. Morbidity and Mortality Weekly Report 53(SS07): 1–57. Available online at: *http://www.cdc.gov/mmwr/preview/mmwrhtml/ss5307a1.htm* (February 8, 2005).

Appendixes

Appendix A

Workshop Agenda

WORKSHOP ON OWNER-AUTHORIZED HANDGUNS

National Academy of Engineering

Green Building
Room 104
2001 Wisconsin Ave., NW
Washington, D.C.

June 7, 2002

7:30 a.m. Continental Breakfast

8:00 a.m. Welcome and Introductions

- *Lance Davis, National Academy of Engineering*

Plans for the Day

- *Greg Pearson, National Academy of Engineering*

Session 1: Technology for Owner-Authorized Handguns
Moderator: *Dixon Dudderar, Lucent Technologies (emeritus)*

8:30 a.m. Keynote Addresses

- *Donald Sebastian, New Jersey Institute of Technology*
- *John Wirsbinski, Sandia National Laboratories*

9:15 a.m. Panel
- *Ken Green, National Shooting and Sports Foundation and Sporting Arms and Ammunition Manufacturer's Institute*
- *Kevin Foley, Smith & Wesson*
- *Peter Sebelius, Charles Stark Draper Laboratory*
- *Naeem Zafar, Veridicom*
- *Wendy Howe, National Institute of Justice*

10:00 a.m. Q&A

10:30 a.m. Break

Session 2: Liability Concerns
Moderator: *Mark Behrens, Shook, Hardy & Bacon L.L.P.*

10:45 a.m. Keynote Address
- *David Fischer, University of Missouri*

11:15 a.m. Panel
- *Larry Keane, National Shooting Sports Foundation*
- *Arthur Bryant, Trial Lawyers for Public Justice*
- *Dennis Henigan, Brady Center to Prevent Gun Violence*
- *Additional panelist TBD*

12:00 p.m. Q&A

12:30 p.m. Lunch

Session 3: Impact on Health and Crime
Moderator: *Lance Davis*

1:30 p.m. Keynote Address
- *Phil Cook, Duke University*

2:00 p.m.	Panel • *Charles A. Moose, Montgomery County Department of Police* • *Paul H. Blackman, National Rifle Association* • *Tom Diaz, Senior Policy Analyst, Violence Policy Center* • *Lois Mock, Department of Justice*
2:45 p.m.	Q&A
3:15 p.m.	Comments from Invited Guests Moderator: *Lance Davis, NAE*
4:15 p.m.	Summary and Closing Remarks *Lance Davis, NAE*
4:30 p.m.	Adjourn

Appendix B

Committee Biographies

LANCE A. DAVIS, *chair*, is executive officer of the National Academy of Engineering (NAE), where he is responsible for the program, financial, and membership operations of the academy; he reports directly to the NAE president. Prior to joining NAE, Dr. Davis was deputy director, Defense Research and Engineering (Laboratory Management and Technology Transition), at the Pentagon from 1994 to 1999. In this capacity, he exercised oversight responsibility for the $11 billion U.S. Department of Defense (DOD) laboratory system and the dual-use and technology-transfer activities of the agency. Dr. Davis spent the majority of his career in industry at Allied-Signal Inc. He joined the then Allied Chemical as a research scientist in 1968 and moved through a succession of management positions, leading to appointment as vice president of corporate research and development in 1984. He continued in this capacity until joining DOD in 1994. Dr. Davis graduated Summa cum Laude from Lafayette College in 1961 with a B.S. in metallurgical engineering. He received an M.Eng. in 1963 and a Ph.D. in engineering and applied science from Yale University in 1966. Dr. Davis is a member of Phi Beta Kappa and Tau Beta Pi. He was elected to NAE in 1992 and received the Defense Manufacturing Excellence Award from the Multi-Association Industry Affordability Task Force in December 1999.

LOUIS F. BEHLING was range foreman at Picatinny Arsenal, a joint-service armament research and development (R&D) center, from 1977 until his retirement in 1995. In that position, he was responsible for all

phases of small-caliber ammunition and weapons, including testing, personnel management, physical security, hazardous materials, scheduling and coordination of test programs, job estimates, modification/design of required test fixtures, assistance to engineering staff in design of test requirements/programs, and travel to various contractors/military locations to help resolve problems with testing or investigations of malfunctions. From 1967 to 1977, Mr. Behling was proof technician and assistant range foreman at Rock Island Arsenal, in Rock Island, Illinois, where he performed testing of experimental and production weapons and ammunition. During his career, he has worked with a variety of firearms, including the M1, M14, and M16 rifles and the M1911A1 and M9 pistols. From 1963 to 1965, Mr. Behling was a member of the Fort Benning Rifle Team, 3rd U.S. Army Rifle Team, 1st Cavalry Division Rifle Team (Korea), 8th U.S. Army Rifle Team, and USARPAC Division All Army Rifle Team. He maintains an extensive cartridge collection dating from the Revolutionary War.

RICHARD L. COSTELLO is retired director of special projects for Colt's Manufacturing Company. Mr. Costello has a broad background and hands-on experience with program management, product design and engineering, manufacturing engineering, and quality assurance in the gun industry. From 1991 until his retirement in 1995, he was director, special projects, for Colt's, where he was responsible for the development of advanced R&D concepts and special product design and manufacture. In a 32-year career with Colt's, Mr. Costello held positions of manufacturing engineer, manager of engineering services, vice president for quality assurance, and vice president for product engineering and quality assurance. Prior to his work for Colt's, he worked as a producibility engineer at Pratt & Whitney Machine Tool Company and a process engineer at Winchester-Western Division, Olin-Mathieson Chemical Corporation. Mr. Costello has B.S./B.A. degree from the University of Hartford.

T. DIXON DUDDERAR is a Distinguished Emeritus Member of the Technical Staff of Bell Laboratories, Lucent Technologies. Dr. Dudderar earned his B.S.M.E. from Lehigh University, his Sc.M. from New York University, and his Ph.D. from Brown University. His areas of technical specialization include experimental studies of the mechanics of materials (including fatigue and fracture, micromechanics, and fluid dynamics); coherent optical metrology (holointerferometry, laser speckle velocimetry, etc.); optical fiber processing; applications of fiberoptics in remote sensing;

high-level microelectronic integration; and electronic packaging for high-reliability, lost-cost manufacture, from initial product design through final qualification. Dr. Dudderar was a distinguished member of the technical staff at Lucent Technologies/Bell Laboratories (formerly known as AT&T Bell Laboratories, and before that simply Bell Telephone Laboratories). He first joined the company in 1958 as an engineer responsible for the design of the first-generation solid-state transponder packages and airborne antenna structures for anti-ICBM defense systems, as well as the horizontal drive system for the AT&T ground antenna for Telstar, the world's first nonmilitary communications satellite. Dr. Dudderar has published more than 60 research papers and been awarded more than 30 patents.

LAWRENCE C. KRAVITZ is retired vice president of technology, Corporate Research and Technology, AlliedSignal Inc. Dr. Kravitz has worked as an engineer and manager in both the private and public sectors. From 1990 until his retirement in 1996, he was vice president, corporate research and technology, for the aerospace, automotive, and engineered materials company, AlliedSignal Inc. (called Honeywell since the 1999 merger of the two companies). Dr. Kravitz was vice president of technology for Allied's Bendix Aerospace Sector from 1986 to 1990. He directed the Bendix Corporate Research Laboratory from 1981 until it was acquired by Allied in 1985. His government career included nine years of service with the Air Force Office of Scientific Research, including four years as its director. Dr. Kravitz has a Ph.D. in applied physics from Harvard University, an M.S. in electrical engineering from the Air Force Institute of Technology, and a B.A. in electrical engineering from the University of Kansas. He has served as an advisor for a variety of government and private organizations.

DAVID MAHER, chief technology officer of InterTrust, has extensive expertise in secure computing. Before joining InterTrust in 1999, he was chief scientist for AT&T Secure Communications Systems, head of the Secure Systems Research Department, and security architect for AT&T's Internet services platform. After joining Bell Labs in 1981, Dr. Maher developed secure communications, information vending, and e-commerce systems. He was chief architect for AT&T's STU-III secure voice, data, and video products used by the White House and U.S. Department of Defense for top secret communications. In 1992, Dr. Maher was made a Bell Laboratories Fellow in recognition of his work on secure communications. He holds multiple patents in secure computing; has published papers on com-

binatorics, cryptography, number theory, signal processing, and electronic commerce; and has been a consultant for the National Science Foundation, National Security Agency, National Institute of Standards and Technology, and Congressional Office of Technology Assessment. He is a coauthor of the recent National Research Council report, *Embedded Everywhere: Network Systems of Embedded Computers* (National Academy Press, 2001). Dr. Maher holds a Ph.D. in mathematics from Lehigh University and has taught electrical engineering, mathematics, and computer science at several institutions.

KAREN WEIL MARKUS, president of Zeus Strategies, LLC, is experienced in business and technology management and has technical expertise in microelectromechanical systems (MEMS) technologies. Zeus Strategies, LLC, is a consulting company focused on corporate technology strategies, mergers and acquisitions, and disruptive technologies. From 2000 to 2003, she was vice president, technology strategy, for JDS Uniphase Corporation. Prior to that, Ms. Markus was vice president and chief technical officer for Cronos Integrated Microsystems, Inc., a MEMS research and development company acquired by JDS Uniphase in 2000. She was chairman of the board and executive director of the HI-MEMS Alliance in Research Triangle Park, North Carolina, from 1993 to 1997; from 1992 to 1999, she was director of the MEMS Technology Applications Center at MCNC, a family of private, nonprofit corporations created to drive technology-based economic development and job creation throughout North Carolina. From 1984 to 1989, Ms. Markus was a staff engineer for TRW Space and Defense Sector in Redondo Beach, California.

Ms. Markus is a member of the National Research Council Panel on Sensors and Electron Devices and has been a member of several other National Academies study groups, including the Committee on Advanced Materials and Fabrication Methods for Microelectromechanical Systems. Ms. Markus has a B.S. in electrical engineering from the University of Southern California, Los Angeles, and has participated in a number of management training programs, including the Executive Program in Corporate Strategy at the MIT Sloan School of Management.

JAMES J. MATTICE is director of management/organizational development at Universal Technology Corporation, an aerospace engineering and management company in Dayton, Ohio. In that capacity, he provides corporate leadership in strategic planning and new business development. He

also supports ongoing government and commercial activities in research, development, technology advocacy, technology transition, executive development, and training. Mr. Mattice's previous positions include Air Force Executive-in-Residence at the Federal Executive Institute, Charlottesville, Virginia; deputy assistant secretary of the Air Force for research and engineering; executive director in the Office of the Commander, Aeronautical Systems Center (ASC); director of development planning, ASC; and a variety of senior management jobs in Air Force laboratories at the ASC, Wright-Patterson Air Force Base, Ohio. Mr. Mattice has 38 years of experience conducting in-house laboratory research and providing leadership in all aspects of basic research, exploratory, advanced development, manufacturing technology, and executive development programs. He has served on numerous boards, special study panels, and advisory committees in government, industry, and academia in the United States and abroad.

LAWRENCE O'GORMAN is a distinguished member of the technical staff of Avaya Laboratories Research, where he works in areas combining digital signal processing and security. Previously, he was chief scientist and co-founder of Veridicom, Inc., a developer of personal fingerprint-authentication systems, and before that he was a distinguished member of the technical staff at Bell Laboratories, Murray Hill, New Jersey. He has worked in areas of pattern recognition and image processing applied to biometrics, security, digital libraries, Web messaging, document processing, and machine vision. Dr. O'Gorman has written more than 50 technical papers and several book chapters and is the owner of 15 patents. He is co-author of *Practical Algorithms for Image Analysis* (Cambridge University Press, 2000) and *Document Image Processing* (IEEE Press, 1997). He is a principal author of two standards, *NIST CBEFF* and *AAMVA/ANSI Common Minutia Template Standard*, and contributor to BioAPI and ANSI X9.84. He is a fellow of the IEEE and the International Association for Pattern Recognition. Dr. O'Gorman is on the editorial boards of four journals and a member of several technical committees, including the National Research Council Assessment Board for the National Institute of Standards and Technology. He received B.A.Sc., M.S., and Ph.D. degrees, all in electrical engineering, from the University of Ottawa, University of Washington, and Carnegie Mellon University, respectively.

LAURENCE C. SEIFERT, vice president, communications products sourcing and manufacturing, at AT&T since 1989, is responsible for

manufacturing and sourcing for AT&T's communications products, including PBXs, key systems, and business telephones units serving business customers. Previously, Mr Seifert held a variety of positions at AT&T, including vice president of engineering, vice president of manufacturing research and development at the firm's Engineering Research Center in Princeton, New Jersey, and director of engineering at the company's Oklahoma City Works and Merrimack Valley Works in North Andover, Massachusetts. He began his career at AT&T in 1957 at Western Electric's Kearny Works in Kearny, New Jersey, and has held various engineering, manufacturing, and product-planning positions at a number of facilities at Western Electric. Mr. Seifert holds a B.S. in electrical engineering from the New Jersey Institute of Technology.

MARVIN H. WHITE is Sherman Fairchild Professor of Electrical Engineering and director of the Sherman Fairchild Center at Lehigh University. The focus of his research is the analysis, design, characterization, and modeling of solid-state electronic devices, sensors, and custom semiconductor integrated circuits for advanced systems applications. With the exception of a short term (1995–1996) as program director, solid state and microstructures, in the Electrical and Communications Systems Division at the National Science Foundation and as a visiting research scientist at the Naval Research Laboratory Solid State Device Branch (1987–1988), Dr. White has been at Lehigh since 1981. Previous to that, he was an advisory engineer at Westinghouse Electric Corporation's Solid State Laboratory Space and Defense Center, Advanced Technology Laboratories, in Baltimore, Maryland. He has a B.S.E. in physics and mathematics and an M.S. in physics, both from the University of Michigan, and a Ph.D. in electrical engineering from Ohio State University. Dr. White has 27 U.S. patents to his credit, has written or co-written more than 200 papers, contributed to four books, and is a member of the National Academy of Engineering.

Appendix C[1]

NIJ-Funded Research on User-Authorized Handguns

[1]These one-page summaries appeared originally on the NIJ website *(www.ojp. usdoj.gov/nij)*.

NIJ-FUNDED RESEARCH ON USER-AUTHORIZED HANDGUNS

RESEARCH PORTFOLIO

Award Title: The Application of Frequency Based Coding to ASmart Gun@ Technology
Award Number: 2002-IJ-CX-K006
Awardee: Technology Next, Inc.
Awardee Contact: Irene Vershinin
Address 25 Manor Drive, #14H
Newark, NJ 07106
Phone Number: (973) 351-8693
Date Awarded: 04/11/02
End Date: 05/31/03
Original Funds: FY 2002: $175,856
Grant Status: OPEN
NIJ Office: Office of Science and Technology
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Newark, New Jersey
Project Description:
FY 02: Prior to receipt of this award, Technology Next designed a frequency based coding technology, which is optimized for security and identification signal transmission. This technology enables designs, which significantly improve signal reliability in unpredictable environments, drastically decrease power consumption and eliminate the threat of replication and jamming.
The aim of this project is to produce a working engineering model of the Asmart gun@ authorization system that could be integrated with typical handgun designs. Their approach is to use frequency based coding for recognition, which is housed in a ring worn by the officer. At the current stage of development, the design shows that the size, weight and power consumption requirements for a law enforcement weapon can be satisfied.
To prove the functionality and reliability of the system, Technology Next will conduct testing in various field situations, environmental hazards and under a number of sophisticated technological threats.
Date Last Modified: 11/15/02
Final Report Received From Grantee: No

RESEARCH PORTFOLIO

Award Title: The Development of an Authorized User-Only Handgun
Award Number: 2002-IJ-CX-K004
Awardee: Smith & Wesson Company
Awardee Contact: Kevin Foley
2100 Roosevelt Avenue
Springfield, MA 01102
Phone Number: (413) 747-3321
Date Awarded: 04/04/02
End Date: 12/31/04
Original Funds: FY 2000: $300,000
FY 2001: $1,767,595
FY 2002: $994,733
Grant Status: OPEN
NIJ Office: Office of Science and Technology
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Springfield, Massachusetts

Project Description:
FY 00: Prior to receipt of this award, Smith & Wesson designed and built electronically fired prototype pistols that include both pin code and fingerprint user access control. However, the size of the circuit board with current fingerprint identification technology is too large to fit inside a handgun; the fingerprint system is contained in a separate module. Therefore, this funding provides for the engineering analysis and design work required to reconfigure the original pistol prototypes into a production worthy design.
FY 01: Smith & Wesson built and started testing 50 next-generation electronic fire/pin code access control prototypes. Research was conducted into a non-fingerprint biometric technology that has the potential for miniaturization to the degree that a completely integrated biometric access controlled handgun can be designed.
FY 02: Smith & Wesson will complete testing the 50 electronic fire/pin code access control prototypes, determine the viability of the non-fingerprint biometric technology and miniaturize the fire control electronics to provide space for the addition of onboard biometric access control.
Date Last Modified: 11/15/02
Final Report Received from Grantee: No

RESEARCH PORTFOLIO

Award Title: Optical Methods for Authorized handgun User Recognition

Award Number: 2002-IJ-CX-K012
Awardee: Exponent, Inc.
Awardee Contact: Dr. Phillip Whitely
4101 SW 71st Avenue
Miami, FL 33155

Phone Number: (305)-661-1000
Date Awarded: 09/30/02
End Date: 09/30/04
Original Funds: FY 2003: $88,810
FY 2004: $98,768
Grant Status: OPEN
NIJ Office: Office of Science and Technology
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Miami, Florida
Project Description:
FY 03: The National Institute of Justice (NIJ) has been working since 1994 to promote the development of Asmart gun@ technologies that will reduce deaths and injuries resulting from the use of weapons taken from law enforcement officers. This project proposes a spectroscopic approach in which a key spectral aspect of a compound is detected to enable only the authorized user the ability to use the handgun. Conceptual designs will be completed in which the various chemicals, spectroscopic and electronic component availabilities and compatibilities will be evaluated in light of practical implementation restrictions to determine workable concepts.
FY 04: Leading design concepts will be prototyped and iteratively tested in a handgun mock-up which will allow optimization of detection criteria and placement of the detector on a handgun. The final optimized concepts will be demonstrated by using the activation of a laser sight to indicate authorized user recognition.
Date Last Modified: 11/14/02
Final Report Received From Grantee: No

RESEARCH PORTFOLIO

Award Title: Creation of a ASmart Gun with Radio Frequency Identification@
Award Number: 2002-IJ-CX-K021
Awardee: Metal Storm
Awardee Contact: Name: Arthur Schatz
Address: Suite 810
4350 N Fairfax Drive,
Arlington, VA, 22203
Phone Number: 703-248-8218
Date Awarded: 9/30/02
End Date: 4/30/03
Original Funds: FY 2002: $185,000
Grant Status: OPEN
NIJ Office: Office of Science and Technology
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Arlington, Virginia
Project Description:
VLe Small Arms (VLe) proposes to develop a detailed plan that would describe how their totally electronic firearm could be revolutionary for law enforcement applications. Their unique firearm, called AMetal Storm,@ is in the prototype stage and was developed over a number of years. The firearm is capable of firing multiple rounds in very close succession to vary lethality. While the firearm is unique, it still needs some development to make it Asmart,@ so that it can properly identify the authorized users. The current design uses a radio-frequency signal that the authorized user sends to the weapon. A receiver on the gun confirms that the signal matches and the gun is then electronically turned on. In this project, VLe plans to examine various other types of Aauthorizing@ technologies to determine which one(s) might be better suited for incorporation into their firearm.
Date Last Modified: 11/06/02
Final Report Received From Grantee: No

RESEARCH PORTFOLIO

Award Title: Firearm Research and Review of Biometric Technologies
Award Number: 2002-IJ-CX-K002
Awardee: iGUN
Awardee Contact: Jonathan Mossberg
1871 Mason Avenue
Daytona Beach, FL
Phone Number: (386)274-5882
Date Awarded: 1/18/02
End Date: 9/30/02
Original Funds: FY 2002: $368,572
Grant Status: OPEN
NIJ Office: OST
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Daytona Beach, FL
Project Description:

iGun Technology Corporation (ITC), a subsidiary of Mossberg Group LLC, will research the adaptability of current and evolving biometric technology for incorporation into a firearm. iGun is teamed with West Virginia University=s Department of Biometrics, Morgantown, West Virginia.
The grant is to begin research on which biometric technology is most adaptable to firearms with the goal of building the most reliable and seamless personalized firearm (Asmart gun@). iGun will take lessons learned from Mossberg=s development of it=s personalized shotgun and determine which biometric technology can withstand the explosive platform a firearm offers

Date Last Modified: 01/07/03
Final Report Received From Grantee: No

RESEARCH PORTFOLIO

Award Title: SafeGun Technology
Award Number: 2001-IJ-CX-K017
Awardee: FN Manufacturing, Inc.
Awardee Contact: Jeffrey R. Rankin
797 Clemson Road
Columbia, SC 29229
Phone Number: (803) 736-0533
Date Awarded: 09/30/01
End Date: 06/30/03
Original Funds: Year: 2002, Amount: $1,034,331
Grant Status: OPEN
NIJ Office: OST
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Columbia, South Carolina
Project Description:

FY01: Phase II developed further advances in the research and development of FN's Secure Weapon System which can be programmed to render the firearm usable only by authorized law enforcement personnel. A Secure Weapon System technology first draft technical specification has been developed. Research findings resulted in directing the engineering model toward an architecture which addresses the concerns of interviewed law enforcement officers, as well as moving from potential causes of system failure.

FY02: Phase III funding will develop a jointly agreed upon definition of the best technology and operational specifications for the Secure Weapon System by investigating emerging technologies for various types of recognition and disconnection systems, building engineering models and assessing practicability with law enforcement agencies.

Phase IV funding will provide final all-inclusive technical report on definition of final design: electronic design, mechanical design, electro-mechanical interface and system integration specifics. Phase IV will also provide a designed, developed and integrated electronic/mechanical prototype representing the combination of selected specifications.

Date Last Modified: 11/15/02
Final Report Received from Grantee: No

RESEARCH PORTFOLIO

Award Title: The Development of A 'Smart Gun "Prototype, Using Handgrip Recognition
Award Number: 2001-IJ-CX-K010
Awardee: Mosermation
Awardee Contact: Jeffrey Moser
4445 Malcolm Avenue
Oakland, CA 94605
Phone Number: (510)635-3024
Date Awarded: 08/30/01
End Date: 07/30/04
Original Funds: FY 2002: $299,510
Grant Status: OPEN
NIJ Office: OST
NIJ Grant Monitor: Miles, Christopher
Topical Category: Firearms Research
Sub-Category: Firearms Research
Policing Technology
Officer Protection and Crime Prevention Technology
Project Location: Oakland, CA
Project Description:
FY 02: Mosermation proposes to develop a prototype weapon that uses the handgrip characteristics of the authorized user as a biometric recognition method. This project will determine the efficacy and feasibility of such a recognition method as a Asmart gun@ technology.
FY03: Testing of the prototype grip recognition system will be conducted on a variety of persons to acquire a wide range of handgrip distribution data. Analysis will be performed to estimate the probabilities of false negatives/positives and then to determine what design and/or engineering requirements will need further development or improvement.
Date Last Modified: 01/07/03
Final Report Received From Grantee: No

Appendix D
Time and Cost Estimate for the Development of a New Conventional Handgun

Assumptions

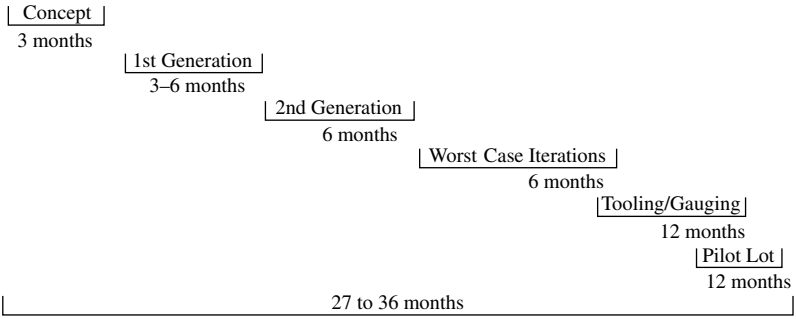
1. Development is aggressive. Normal methods will *double time and cost.*
2. Design is a clean sheet of paper.
3. Design is a single caliber.
4. No significant capital equipment (machinery) needs.
5. Does not include production, labor, materials, and expense.

Methods

1. Design: Solid modeling methods (3D design). Will depict desired fits and clearances prior to modeling, resulting in a somewhat longer design period but a much shorter time for modeling, testing, etc.
2. Dimensional Analyses: Using solid modeling (graphical) instead of computational methods will speed results.

Time and Cost

$3,000,000 to $3,700,00 over a period of 27 months to 3 years, which could lead to production in 33 months to 42 months.



Timeline for development.