SAND REPORT

SAND2001-3499
Unlimited Release
Printed November 2001

“Smart Gun” Technology Update

John W. Wirsbinski

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2001-3499
Unlimited Release
Printed November 2001

Distribution

"Smart Gun" Technology Update

By

John W. Wirsbinski
Systems Analysis and Development Group
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0759

Abstract

This report is an update to previous "smart gun" work and the corresponding report that were completed in 1996. It incorporates some new terminology and expanded definitions. This effort is the product of an open source look at what has happened to the "smart gun" technology landscape since the 1996 report was published.

ACKNOWLEDGEMENTS

Thanks go out to all of people who supplied the information to make this report possible. This report consists of the aggregate ideas of many people who work in, and are knowledgeable about, the law enforcement profession, firearms, and various technologies. Special thanks go to Wendy Howe, at the National Institute of Justice Office of Science and Technology for sponsoring this work and providing information and insight into the "smart gun" technology realm. Additional thanks go to Sandia team members Darren Buie, John Lavasek, Douglas Loy, Kent Pfeifer, and Bill Suderman. Without their efforts this project would not have been possible.

Contents

1.0 INTRODUCTION

This report is an update to previous "smart gun" work and the corresponding report that were completed in 1996. It incorporates some new terminology and expanded definitions. This effort is the product of an open source look at what has happened to the "smart gun" technology landscape since the 1996 report was published. In gathering information for this report, the authors contacted organizations with technologies applicable to this topic and conducted open literature searches. The information collected was organized and condensed into this report. Sandia National Laboratories (Sandia) did not test any technology nor attempt to validate or invalidate any claims. However, where applicable, Sandia has provided insight into scientific and engineering principles that apply to the information collected.

1.1. Background

In May 1996, Sandia published a report titled *Smart Gun Technology Project Final Report*. Those interested in "smart gun" technologies are highly encouraged to obtain and read this report. It is available by calling NTIS at 1-800-553-6847. It is also available in an electronic, PDF format at http://infoserve.sandia.gov/sand_doc/1996/961131.pdf.

The 1996 report was the result of approximately 22 months of research. This effort had three objectives: find and document user requirements for a "smart gun"; investigate, evaluate, and prioritize technologies that may meet the requirements for a "smart gun"; and demonstrate and document the strengths and weaknesses of various technologies as applied to the "smart gun" concept.

The 1996 report and the current research and report were produced at the request of the National Institute of Justice (NIJ) Office of Science and Technology (OST). As the technology research agency of the Department of Justice, NIJ/OST provides federal, state, and local law enforcement and corrections agencies access to the best technologies available and helps them develop capabilities essential to improving efficiency and effectiveness. One area of concern with respect to officer safety is officers killed every year by their own weapon. The previous research that resulted in the 1996 report was an attempt by NIJ to identify a technological solution to this officer safety problem. The current report updates the status of technology development that is applicable to the "smart gun" concept.

Sandia National Laboratories is a Department of Energy multiprogram science and engineering research and development facility. Sandia currently supports the OST network of National Law Enforcement and Corrections Technology Centers (NLECTC) by operating the Border Research and Technology Center, the Center for Civil Force Protection and the Public Safety Technologies Assessment Facility. The NLECTC provide research and technology implementation support to state and local law enforcement agencies around the United States. Through the Public Safety Technology Assessment role, Sandia is able to provide unbiased, science and technology-based assessment and evaluation of proposed "smart gun" technologies.

Since the 1996 "smart gun" technology report was written, several firearms manufacturers, including Colt's Manufacturing, have used internal and/or government funding to develop "smart gun" technologies. This includes multiple manufacturers of other technologies, as well as small-scale inventors, who are actively pursuing the development of a "smart gun". In addition, there have been recent legislative efforts to mandate the implementation of "smart gun" technology. A number of jurisdictions are researching the feasibility of "smart gun" technology.

This report is intended to update the 1996 report to ascertain the current status of "smart gun" development and provide agencies with information that will help with their assessments of "smart guns".

1.2. Scope of Work

The scope of this report is limited and is the result of approximately two months of effort. The effort relies upon open source documentation and information from companies engaged in the development of "smart gun" technologies. Sandia made an attempt to be thorough in contacting organizations, but it is possible that applicable technologies have been missed.

This report relies upon the 1996 requirement as still being an accurate representation of the needs of the law enforcement community. However, Sandia did make limited contact with the law enforcement community. Most of this contact was to understand the types of evaluations they are being asked to perform with respect to "smart guns" to ensure that this report will be valuable to the law enforcement community.

The 1998 and 1999 FBI Uniform Crime Reports: *Law Enforcement Officers Killed and Assaulted* (the most recent reports available) were reviewed. They can be found at http://www.fbi.gov/ucr/ucr.htm. These reports confirm the continued existence of a problem associated with officers being disarmed and killed by their own service weapon.

This document, like its predecessor, is focused on "smart gun" technology as applied to law enforcement handguns. It does not address the issues of safe storage of weapons (e.g., in the home). It also does not address the application of "smart gun" technology to other types of weapons such as rifles or shotguns. Finally, the evaluation of technologies and/or approaches is being conducted from the perspective of the law enforcement officer requirements documented in the 1996 report. This report does not extensively address the applicability of technologies to the needs or desires of a civilian commercial market (See Appendix B).

1.3. Objectives of This Work

This effort had two objectives. The first objective was to document the current status of technologies that may be applicable to the development of a "smart gun". Sandia reviewed the technologies identified in the 1996 report as well as new ideas that are being promoted by industry. Like the 1996 report, the capabilities of these technologies are being compared against the law enforcement user requirements.

The second objective is to provide information to the law enforcement community that will assist them in understanding the concept of a "smart gun" as well as the technologies being pursued as potential solutions. This report should provide law enforcement officers with enough understanding that they can make their own informed assessment of the value particular approaches and/or claims regarding "smart guns" and "smart gun" technologies.

1.4. Research Approach

Several researchers conducted this effort. The researchers conducted open literature searches. From these searches, organizations and technologies were identified that were involved in the development of "smart guns". The Sandia researchers attempted to contact the organizations and asked them to provide information on the status of their work with "smart guns". The organizations were informed to only provide information that they were willing to have released

in a public document. Sandia researchers followed up on the information as necessary. The information gained from the open literature searches, the organizations, and engineering judgement was integrated and forms the basis of this report.

1.5. Definitions

This report deviates in one significant respect from the 1996 report: the definition of "smart gun". Because of the legislative efforts and the politicization of the "smart gun" concept, this document is defining the term "smart gun" as an overarching concept, as opposed to a particular technological solution. This document will also provide definitions for other subcategories of the "smart gun" concept that define weapons that may meet a subset of those requirements. These definitions will provide a means of categorizing technologies and assist law enforcement officers with evaluating products and/or technologies being advertised as "smart guns".

1.5.1. Authorization Terminology

In the 1996 report, Sandia used the analogy of a padlock and key to describe the concept of the "smart gun". To expand upon this, this report uses terminology from security and access control. The three terms described below are used to describe the type of identifier used to ascertain an individual's authority to access something, or in the case of "smart guns", discharge the weapon.

1.5.1.1. Something a Person Knows

This term refers to authorization granted based upon knowledge possessed by the individual. Examples of knowledge-based authorization are systems that use things like combinations, personal identification numbers, and passwords.

1.5.1.2. Something a Person Has

This term refers to authorization granted based upon something that is possessed by the individual. The credential is actually what is recognized and authorized, but with strict control of the credentials, the system in effect authorizes individuals. Examples of credential-based authorization are systems the utilize things like tokens, magnetic stripe badges, and proximity cards.

1.5.1.3. Something a Person Is

This term refers to authorization granted based upon some unique, inherent physical trait. This type of authorization utilizes biometrics, i.e.; detection and measurement of one or more of a person's unique biological characteristics, to ascertain the identity of the individual. Examples of biometrics-based authorization devices are systems that utilize voice recognition, hand geometry, iris scans, and fingerprints.

1.5.2. Weapon Technology Categories

The following paragraphs will describe the categories into which the technologies will be grouped. The definitions will include both a definition of the category and identification of the type of authorization most likely to be associated with technologies in the particular category.

1.5.2.1. Mechanical Safety

This is a device that prevents the gun from firing until a lever or other mechanical mechanism is moved or manipulated. There is no unique identification provided by this capability. These

devices are intended primarily to help prevent accidental discharges. This category uses knowledge-based authorization exclusively. Furthermore, the knowledge is not of a unique identifier, so this type of mechanism does not provide any discrimination between an authorized and an unauthorized user. These items are common and found on many firearms in use today. Examples of mechanical safeties include safety levers on weapons, push button safeties, magazine disconnects, and firing pin blocks.

1.5.2.2. Lockable Gun

A lockable gun is one that has an integral mechanism that prevents the locked firearm from being discharged until an authorized user is recognized. A lockable gun requires an overt action by the user to both lock and unlock the firearm (i.e., once unlocked the firearm can be fired by anyone until it is re-locked). The locking mechanism may be mechanical, electromechanical, or electronic. The authorization can be by something known (e.g., combination) or something possessed (e.g., key). Examples of locking guns or devices to turn a standard gun into a locking gun are available and marketed.

1.5.2.3. Self-locking Gun

Self-locking guns are designed to be fired only by an authorized user. These weapons, as the name implies, automatically reverts to a locked state when a proper firing grasp of the weapon is released. These weapons may or may not re-authorize the user between shots. These guns do not require the user to perform any action to re-lock the weapon other than removing the weapon from the firing grip. A self-locking gun recognizes authorized users by either something known, something possessed, or some characteristic unique to the user. It may or may not require the authorized user to perform a conscious action (beyond grasping the weapon) to enable the weapon. The locking mechanism can be mechanical, electromechanical, or electronic. Examples of self-locking gun concepts do exist and are marketed, but they are currently mostly a specialized retrofit to certain existing weapons or are incorporated in the products of small, specialty manufacturers.

1.5.2.4. Personalized “Smart Gun”

For this report, a personalized smart gun is defined as one that is designed to be fired only by an authorized user and which has a mechanism that automatically authorizes the user and also automatically reverts to a locked state. A personalized smart gun authorizes firing based upon an inherent characteristic of the individual (biometrics). The locking and unlocking is transparent to the user and does not require any overt action (beyond grasping the weapon) and does not require any type of external device. The weapon is at least as reliable as today’s high quality weapons and the system identifies the user between shots without interfering with the speed at which the shooter can pull the trigger and fire the weapon. The locking mechanism may be mechanical, electromechanical, or electronic. It also must function in all environments and work whether the user holds the weapon with a single hand (either one), or two hands. It must recognize the user whether the user is wearing gloves or there are fluids or dirt on the hand or gun. An example of a personalized “smart gun” that meets this description is unknown to Sandia at this time. Appropriate technologies are likely to involve some type of biometrics device.

1.5.2.5. "Smart Gun"

"Smart gun" is a phrase used throughout this document to generalize the concept of weapons that have some level of use authorization capability. The term "smart gun" encompasses lockable guns, self-locking guns, and personalized "smart guns".

1.5.2.6. External Locking Devices

There are numerous external locking devices on the market that prevent the firing of a weapon by enclosing part of or the entire firearm. These devices include things like trigger locks and gun lock boxes. These external devices are not readily applicable to the on-duty officer. They may have some applicability to the safe storage of the weapon while it is not being carried, but that is outside of the scope of this document. An additional type of external locking device is the locking holster, including the soon to be released personalized retention holsters that use biometrics (fingerprints) to identify authorized users. However, since these only prevent (or reduce) the likelihood of a weapon being taken away while it is holstered, they are at best a partial solution. Given this partial solution nature, they are not considered in this report. These external devices are mentioned because legislative attempts and some efforts at evaluating "smart gun" technology have addressed devices of this nature. Hence, they are included cursorily to acknowledge the relevance of these items to "smart gun" discussions.

2.0 "SMART GUN" REQUIREMENTS

Sandia and NIJ agreed to use the requirements identified in the 1996 report for this evaluation as well. This consistent set of requirements provides continuity between the two reports. From an analysis standpoint, any comparisons between the evaluations of technologies in this report and the 1996 report will be simplified, because the requirements have remained unchanged. A summary of the requirements from the 1996 report is in Appendix A.

The weapons need to be reliable in all of the environments in which an officer must operate. This need is reflected in the observation that all, or nearly all, attempts to legislate the development and marketing of a "smart gun" exempt law enforcement and sales to law enforcement from the requirements. Given this situation, it is likely that any requirement identification efforts would result in requirements similar to those identified in 1996.

2.1. "Smart Gun" Use Scenarios

One way of condensing the functional requirements for "smart guns" identified in the 1996 report into a useable form is to generate scenarios incorporating these requirements. This approach is not as thorough as a fully documented requirements list. However, it is easier to relate to for users and complements the requirements based approach.

For the "smart gun" requirements for law enforcement, Sandia has identified two primary scenarios. These scenarios are generic, but reflect the type of situations in which an officer's weapon is taken and used to injure the officer, other officers, and/or the public. In addition, Sandia has included 2 additional scenarios that are related to the requirements, but are only peripherally related to the common types of scenarios in which a law enforcement officer's weapon is taken and used malevolently. These scenarios were used as operational reflections of the functional requirements during the review and assessment technologies for this report.

2.1.1. Scenario 1 (Primary)

During an interaction with an officer, the perpetrator removes the officer's weapon from the holster. This action is done through either stealth or force. The perpetrator should not be able to discharge the weapon. This scenario could occur in many different environments. These environments include, but are not limited to, booking suspect at police station, traffic stop, domestic violence call, and prisoner transport.

2.1.2. Scenario 2 (Primary)

During an interaction with a perpetrator, the officer has justification to draw his sidearm. A struggle ensues and during the struggle the offender gains control of the officer's weapon. The perpetrator should not be able to discharge the firearm. Note that it is assumed that it is unlikely that the perpetrator can turn the gun and cause it to discharge (hitting the officer) while the firearm is still in the officer's hand in a completely functional firing grip. This assumption implies that either the officer is in limited contact with the weapon but has lost his primary control and firing grip or that he has no contact with the firearm and has lost complete control of the weapon. This scenario can also occur in many different environments (see Scenario 1).

2.1.3. Scenario 3 (Peripheral)

Two officers (Officer A and Officer B) are at the scene and Officer A requires the use of the Officer B's weapon. In the worst case scenario, Officer B is disabled and Officer A removes the firearm from either Officer B's hand or holster. Officer A should be able to discharge the weapon as an authorized user, without any action on the part of Officer B.

2.1.4. Scenario 4 (Peripheral)

An officer is at his home or other private, trusted location and removes his sidearm from his immediate control. The weapon cannot be fired by a child or unauthorized adult, but it can be instantly fired by the officer when he picks it up.

2.2. Update to 1996 "smart gun" Report Requirement

This report does not try to revisit all of the requirements in the 1996 report. However, on page 80 of the report, the last requirement has generated some questions that deserve clarification. The requirements states that, "The "smart gun" technology system must operate during and after exposure to radio frequency interference." The value of concern is the high frequency target value, "130 dBm > 100 MHz." This value was obtained from a military requirement for an advanced development sidearm. While it is uncertain as to the specific operational environment to which this requirement relates, it is extremely stringent relative to the typical law enforcement officer's operational environment. This value may refer to a shipboard environment with high power radar and extensive electronics; however, the requirement exceeds the needs of the law enforcement user. To come up with a value that is more appropriate, the electromagnetic interference (EMI) values used by car manufacturers were reviewed. Some car manufacturers test for EMI problems in accordance with international EMC standards. One manufacturer has tested their vehicles with transmitters with a frequency range from 1.8 MHz to 1 GHz, using 10 different antenna locations. The manufacturer requires that the vehicle performance shall not be affected by transmitters in the 200-W range, and that no system in the car shall be damaged by a field strength of up to 200 V/meter. Taking into consideration that an officer's vehicle is likely to encounter most, but not all of the same environments as the officer's weapon, a conservative,

but reasonable, approach is to double the vehicle requirement. Thus, a "smart gun" must operate unaffected in an EMI environment containing 400 V/meter electromagnetic radiation in the 1.8 MHz to 1 GHz values.

3.0 CURRENT ACTIVITY RELEVANT TO "SMART GUNS"

Currently there is a significant amount of activity in the "smart gun" arena. This activity ranges from research and development to state and federal attempts at legislation. This section provides a brief overview of some of these activities. This overview will provide the reader with a context in which to place the technology evaluations.

3.1. Legislative Activities

The first area of activity to be discussed is the legislative activity surrounding the topic of "smart guns". Several states have introduced legislation mandating that all guns sold in the state after a certain date must be "smart guns". As noted previously, in general these proposed laws exempt law enforcement officers from this requirement. To date, none have passed, though several state legislatures have created committees or funded organizations to research the feasibility of "smart gun" technology (e.g., Maryland, New Jersey, and New York). In addition, states have passed mandatory storage legislation and mandatory trigger lock legislation. Maryland has also passed legislation that requires firearms manufactured after a certain date and sold in Maryland incorporate some type of integral locking mechanism (See definitions, locking gun). In addition to attempts at legislation, individuals have attempted to sue gun manufacturers for negligence in not producing intelligent weapons and thereby creating unsafe products.

3.2. Manufacturer Agreements

One result of the lawsuits and threatened lawsuits has been attempts by the federal and some city governments to establish agreements with gun manufacturers to get the manufacturers to voluntarily incorporate internal locking mechanisms and/or authorized user technologies by certain dates. These agreements have also attempted to influence business operations by requiring specific percentages of annual revenues be committed to "smart gun" research and development. Since these agreements are entered into voluntarily, these agreements do not have any influence on other (non-signatory) manufacturers, other than possible political leverage. Very few manufacturers have signed these agreements.

3.3. Philosophical Debates

One result of the efforts to develop intelligent weapons has been the philosophical debates that have ensued as a result. Most people support the conceptual ideal of a "smart gun" (see personalized "smart gun" definition).

However, beyond the conceptual ideal, there is a great deal of variation in support. The media periodically reports on activity in this arena. Most recently, much of the reporting has been related to legislation aimed at mandating this technology.

Pro-gun organizations generally support the ideal of "smart guns". Furthermore, they support research and development into the development of "smart guns" by the federal government and/or industry. However, most do not trust the technology and some are vehemently against any legislation that mandates the incorporation of smart weapons technology. There is a perception that "smart gun" legislation is an indirect attempt to ban firearms by first outlawing

non-"smart guns" despite an inability to manufacture "smart guns", thereby resulting in a defacto ban. Some individuals, organizations, or manufacturers have stated that "smart guns" are less safe because they will promote unsafe storage practices and that they will not provide a meaningful reduction in accidental deaths or suicides because in most cases these individuals will be authorized to fire the weapon. There is also a concern about liability should a false accept or false reject cause a death or injury that the system should have prevented.

3.4. Resulting Activity

The results of this interest, debate, media, and legislative activity are varied. There are numerous efforts to justify or discredit the "smart gun" concept. There are also the efforts by the states, as mentioned in Section 3.1, to create or direct organizations to review and study the "smart gun" concept and make progress. Section 4.0 will discuss some of the technology activities related to "smart guns". In addition, there are efforts to show economical advantages for mandating "smart gun" technology that use questionable economic models and fail to address the technological challenges inherent in creating a "smart gun". Other efforts exist to try to pool public (state and/or federal) resources with the private sector to try to address the technological, economic, sociological, and political/legislative issues associated with "smart guns". The results of these public/private partnerships are unknown because they are still in their infancy. However, they at least appear to be cognizant of many of the issues associated with "smart guns". It remains to be seen whether public and private entities can actually come together and work together to produce valuable results.

All "smart gun" efforts are currently somewhat limited by the lack of a consistent, universal definition of "smart guns". The definition frequently changes either subtly or significantly depending upon the ideology of the speaker. The conceptual user is also subject to change, for example, from homeowner, to police officer, to civilian, to concealed weapons permit holder. These shifting definitions make for difficulties in comparing the data from study to study or research group to research group. Evaluators are cautioned to carefully identify and understand definitions and any pre-existing ideologies prior to utilizing or comparing studies and documentation.

4.0 TECHNOLOGY STATUS

This section will highlight technologies and their applicability to "smart guns". In a departure from the 1996 Sandia report, this document does not provide detailed descriptions of all potential technologies. It focuses on technologies being applied to "smart guns". Furthermore, this report does not provide the technology evaluation and ranking as in the 1996 report, because the inherent ability of particular technologies to meet the requirements has not radically changed. However, what may have changed is the maturity of the technology and/or the technology implementation, and these are addressed in this document.

4.1. Firing Systems

The definitions for the types of "smart guns" do not include the firing system as part of the definitions. However, since the 1996 report was written, there have been some developments in weapons firing mechanisms that may impact "smart gun" development.

Most current firearms fire a bullet using a similar process. The firearm either manually or automatically chambers a cartridge. The cartridge consists of a case, primer (ignition source),

powder (fuel), and a bullet (projectile). When the firearm trigger is pulled, it initiates a mechanical action that results in a strike to the primer. The percussive blow detonates the primer; the detonation ignites the powder; the burning powder generates a gas that propels the bullet.

There are at least two new concepts that partially or entirely modify this firing sequence. The first variation is one in which the percussively activated primer is replaced with an electronically activated primer. In all other ways, this system is comparable to the current firearms. In this type of system the cartridge is essentially unchanged, except for the primer design. In firing the weapon, when the trigger is pulled, instead of a percussive blow, an electrical charge is released into the primer. This charge detonates the primer and subsequent events to discharge the bullet. This type of firing mechanism exists in a commercial product. Currently it is used in a bolt action rifle, which is not typically the primary focus of "smart gun" development. However, there are manufacturers investigating the application of this type of firing system for use in handguns, which are the primary focus of "smart gun" development activities.

The second type of innovative firing system is a radical departure from the traditional firing process. In this system, there no moving parts, no separate magazine, no ammunition feed or ejection system, and no conventional cartridge case. The only things that move are the projectiles. The only operating components are electronic. At the core of the technology is a projectile design, which enables multiple high-pressure projectiles to be stacked in-line in a barrel with gunpowder between each bullet. The powder charges are then electrically fired in sequence, thereby sequentially firing the bullets. This approach results in an operating system that is entirely electronic. This system has been demonstrated in an engineering prototype. Additional research is ongoing and is being funded, in part, by the United States Defense Advanced Research Projects Agency. As a "smart gun" platform, this system provides some unique opportunities. The space typically used for the magazine and bullets is available for electronics. An all-electronic system also has the potential to simplify the interface between the identification, locking, and firing systems. Fewer moving parts reduces the number of parts that can wear out. The lack of a bullet chamber and ejection system eliminates the possibility of many types of jams. Combined together, the result may be a weapon even more reliable than the already highly reliable firearms currently available. However, the ultimate reliability will be determined by the ability of the electronics to withstand environmental conditions and potentially tens of thousands of rounds of ammunition being fired. The potential drawback is that maintenance procedures and operational procedures (especially reloading) will be substantially different than current firearms designs.

4.2. Identification Systems

In assessing technologies for "smart guns", most of the effort has been focused on the identification system. Sticking with the terminology defined in section 1.5, the identification is based upon either something a person has, something a person knows, or something a person is. This terminology is used in conjunction with the definitions of lockable guns, self-locking guns, and personalized "smart guns" to categorize the technologies that were reviewed.

4.2.1. Lockable Guns

Lockable guns are currently the most well developed form of "smart gun". There are several examples of technologies that retrofit to existing firearms and new firearms that are sold in a lockable form.

4.2.1.1. Existing Lockable Guns

Most of the marketed systems rely on either a mechanical key identification system or a combination (generally push button) system. These systems are relatively inexpensive, and they also use systems that are mechanical in nature. Other technologies could be used (e.g., radio frequency (RF) technology with a remote control on/off button) but since these other technologies appear applicable to self-locking guns or perhaps even personalized "smart guns", most efforts have not bothered to use this level of sophistication to achieve only a lockable weapon.

Evaluations by other entities that Sandia reviewed generally concluded that these mechanisms have some desirability, and in some cases been considered for implementation by law enforcement agencies. However, most of the reviews indicate that the value in these systems is in off-duty storage, as opposed to on-duty carry. Most recommended that while on-duty the officer should carry the weapon unlocked because they are slow (relative to an unencumbered draw and shoot scenario) and there is high probability of fumbling the combination or key during a life or death engagement. In terms of the scenarios, these weapons can reasonably fulfill the needs of Scenario 4 and possibly 3, but they are not adequate for Scenarios 1-2.

In addition, the 1996 report ranked lockable gun technologies such as the ones currently being marketed at the bottom of the technologies when scored against the officer generated requirements. This assessment remains valid.

If the primary value of these systems is the safe storage of a weapon in an off-duty environment (primarily the officer's home) it may be that a quick access storage device will provide more benefits[1]. There are multiple examples of devices which are activated using mechanical or electromechanical combination locks and at least one that utilizes biometrics (fingerprints) to open. Because of the greater size of these devices and the more controlled environment of a home, they are likely to be more reliable than a mechanism on a gun that endures multiple environments. In addition, a properly mounted storage box also provides some protection against actual theft of the weapon, whereas a lockable gun can still be stolen and tampered with in another environment. As a result, the lockable gun provides minimal benefits over a quick access storage device in the officer's home. Therefore, assuming that a lockable gun will be carried in an unlocked condition when in a duty situation, the primary value of a lockable weapon is the ability to secure the weapon while it is out of the officer's direct control in a non-home environment.

4.2.1.2. Future Lockable Guns

There is at least one company pursuing a lockable gun that utilizes a different approach than is being currently marketed. This approach utilizes a radio frequency (RF) transmitter to activate

[1] Given the definition used in this document for a lockable gun, both lockable guns and a lock box require an overt action by the authorized user to put the weapon in a secure state.

and deactivate the weapon. This approach was discussed in the 1996 report under the heading of remote control. This approach would be effective for Scenarios 3 and 4. For Scenarios 1 and 2, there is less credibility, especially if the officer is disabled prior to being disarmed. The comments in the 1996 report regarding this approach still apply. For example, a likely operational scenario is one where the officer activates the weapon at the beginning of the shift. Anyone getting control of the weapon can now fire it, unless the officer deactivates the weapon. In this scenario it is highly likely that during a struggle and attempt to retain the weapon, the officer will be unable to deactivate the weapon, and may even forget to attempt deactivation. During a grappling engagement for retention of the weapon it will be nearly impossible for all but the most highly trained individuals to avoid fixating on the weapon retention at the exclusion of all other actions. Another concern is that the control would need to be kept readily available. However, this control is now also readily available to any adversary in close proximity to the officer (for example: a suspect during an arrest attempt). Issues of jamming and radio interference are also concerns.

4.2.2. Self-locking Guns

Self-locking guns represent the focus of most "smart gun" research efforts currently being proposed. They should provide additional security over lockable guns by self-locking. Since they automatically lock, they should generally be able to fulfill the requirements represented by all 4 scenarios identified in section 2.1, though they do not meet all of the requirements for the idealized "smart gun".

4.2.2.1. Existing Self-locking Guns

There are several examples of self-locking guns currently on the open market. In general, these weapons rely upon something an individual possesses to authorize the firing of the weapon. The most common approach currently are weapons that utilize a magnetic ring that when placed in an appropriate location on the weapon, the internal locking mechanism is released, allowing the weapon to fire. Several different companies use this approach. In some cases, the companies sell a custom firearm with this system integral to the weapon. These are small, relatively unknown manufacturers. Currently Sandia does not know of any large scale firearms manufacturers that manufacture or market a weapon incorporating this type of design. The existing sources for these types of designs are companies that sell kits to retrofit to specific weapons. Some of these retrofits can be done by the owner, while others must be done by the company itself.

4.2.2.2. Future Self-locking Guns

As already noted, a great deal of the research being conducted in the area of "smart guns" is focused on self-locking firearms. There has been extensive efforts focused on the development of weapons utilizing RF identification. This focus may be a reflection of the results in Sandia's 1996 report, which identified RF tags as the highest scoring technology. It may also validate Sandia's evaluation. In either case, it remains a promising approach for a future self-locking gun. Colt's Manufacturing aggressively pursued a weapon design based upon an RF tag and produced a prototype, but has since discontinued work on this concept due to technical difficulties and lack of funding. Other companies continue to pursue this approach using similar technologies.

Other companies are actively pursuing "smart guns" that utilize biometrics to ascertain the authorization of an individual. The most common approach is based upon a fingerprint reader. Since the 1996 report, fingerprint-reading technologies have reduced in size significantly. They have also been implemented in access control systems to grant access to networks. This implementation is a step forward, but further miniaturization is needed. The robustness of these types of devices in multiple environments associated with a weapon carried in a holster is also untested. Furthermore, the issues regarding partial or complete fingerprint obscuration due to dirt, blood, damage, and/or gloves are unresolved.

In addition to fingerprint readers, several other biometrics are being investigated. One system is attempting to identify authorized users based upon the pressure points associated with the person's grip of the weapon. The company hypothesizes that this system may even work through thin gloves, such as may be used by some law enforcement officers during driving or frisking a suspect. Conceptually, this approach seems to be extremely feasible for the prevention of accidents involving children. However, it is unknown how precise the hand position must be to have an acceptably low false reject rate to account for thin gloves, changes in hand position while under stress or because of injury, etc. In addition, this identification must occur while retaining an acceptably low false accept rate for people with similar sized hands. It is also unknown if there are any miniaturization issues associated with this technology at this time.

Another biometric being investigated involves an infrared scan of the hand at a subcutaneous level and identifying based upon nerves, muscles, and bone structure. This technology also has the potential to work through thin gloves. Furthermore, the presence of dirt, blood, or minor injuries should not change the hand enough to cause a false rejection. It will also be difficult to defeat because the characteristics are not easily visible. However, it seems likely that insulated gloves would still prohibit identification of the user. The technology has been implemented in a time and attendance device and will soon be used in an access control product. The company expects to have a product for "smart guns" by mid to late 2002.

4.2.3. Personalized "Smart Guns"

Personalized "smart guns" represent the design goals for an intelligent weapon. Currently nothing has been developed that meets the full requirements identified in the 1996 report. In addition, Sandia is currently unaware of any near term technologies that will allow the development of a personalized "smart gun". However, lessons may be learned from the efforts to develop locking guns and self-locking guns that may eventually evolve into a personalized "smart gun". However, at this time personalized "smart guns" do not appear to be likely without several years of research and development efforts.

4.3. Locking Systems

In the 1996 report, Sandia noted that it was the responsibility of each manufacturer to understand the chain of events in their products firing mechanism and identify the most appropriate way to block that chain until a user is authorized. This remains a true statement, and Sandia did not investigate locking mechanisms during this update. However, with the introduction of firearms that use an electronic detonation system instead of a percussive system, a few observations can be made. From a reliability standpoint it is likely that a purely mechanical system is likely to be more reliable than one that interfaces between electronic and mechanical subsystems. Furthermore an entirely electrical system should also be more reliable than an electromechanical

system. With appropriate hardening against simple attacks such as shorting of terminals or removal of the battery, purely electronic locking mechanisms are likely to be more difficult for an adversary to defeat than a purely mechanical system. All of these statements are assuming equivalent levels of engineering and testing. Given this observation, it is likely that the most viable "smart guns" will ultimately utilize an electronic firing mechanism, because of superior locking capabilities and interfacing with the identification subsystems.

5.0 CONCLUSIONS AND RECOMMENDATIONS

In 1996 Sandia published the *Smart Gun Technology Project Final Report* after approximately 22 months of research. That effort included extensive surveys of law enforcement personnel to identify the needs of the officers for a conceptual product called a "smart gun". Since that time, the topic of "smart guns" has become a subject for debate amongst people and organizations with different political agendas. It also has become a politically charged subject as various levels of government have considered legislation calling for the investigation or development of "smart gun" technology. In response, NIJ asked Sandia to update its previous report to identify changes in technology that may have occurred since 1996.

To provide further definition to the issues being discussed in conjunction with the "smart gun" concept, this report subdivides "smart guns" into lockable guns, self-locking guns and personalized "smart guns". The investigation associated with this activity determined that lockable guns are currently available commercially at negligible cost. There is minimal research going on with respect to lockable guns, but some remotely operated RF systems are being investigated. Self-locking guns are also available commercially, but are more of a specialty item that is either retrofitted to a particular existing weapon design or made in small quantities by small, specialty firearms manufacturers. However, most of the "smart gun" research currently underway is focused on self-locking guns. Many of the technologies in these approaches have advanced significantly since 1996 and may be feasible within a few years. The robustness of these solutions remains to be demonstrated, but if the reliability is present, some of the biometrics-based and RF-based systems may meet many law enforcement requirements. However, there is currently nothing that Sandia identified that will provide a near term solution which meets all of the requirements and meets the definition of a personalized "smart gun".

An important development since the 1996 report has been the production of firearms that utilize electronically fired bullets. There are two approaches being investigated. One approach is to utilize cartridges with special primers that are actuated electrically instead of percussively. This approach exists as a commercial product in rifles and should be readily transferable to handguns. The second approach is still in the research phase, but utilizes bullets, with gunpowder between each bullet, stacked in a barrel and electrically activated. There are no cases and no mechanical operations. The potential of electronic activation lies in the simpler interfaces between electronic identification and an electronic locking mechanism. Furthermore, it is probable that a well-designed electronic lock will be more difficult to defeat than a comparably designed mechanical or electromechanical lock. Hence, electronically discharged firearms may ultimately prove to be the preferred platform for "smart guns". However, this can only occur after the systems have proven themselves and users accept firearms built upon an electronic platform.

There have been significant innovations and advancements in technologies that may apply to the development of "smart guns". Furthermore, there is strong interest by numerous entities to see a smart gun developed. However, there is nothing currently available or that appears to be

available in the immediate future that will meet all of the requirements identified in the 1996 report for law enforcement use. This fact is reflected in the observation that all legislation considering the mandating of "smart guns" has exempted law enforcement from the requirements. Furthermore, the current research and expected near term results appear to be capable of generating evolutionary gains and capabilities for self-locking guns, but nothing appears to be approaching personalized "smart guns" in the near-term. Hence, Sandia's current assessment is that it will still take multiple years of dedicated research and development before a personalized "smart gun" will be developed that meets the functional requirements of the law enforcement officer.

APPENDIX A

1996 "SMART GUN" ENGINEERING REQUIREMENTS

Intentionally Left Blank

SCOPE

- A smart gun technology system consists of an interdependent group of keys, discriminators, and latches integrated with a firearm.
- A smart gun technology system must have a unique identifier that can be associated with a user.
- A smart gun technology system must have a means to discriminate between keys.
- A smart gun technology system must have a mechanism to latch the firearm so that it cannot be fired.

PHYSICAL CHARACTERISTICS

- The weight that the smart gun technology adds to the firearm should be less than 3.5 ounces.
- The size that the smart gun technology adds to the firearm should be less than 2 cubic inches.
- The 'addition of the smart gun technology should not change the firearms balance so that the use of the firearm is affected.
- The change in the firearm's shape should not affect its use in existing holsters.

POWER

- The technology used should not need an electrical power source. If a power source must be used it must meet the following power requirements.
- The target value for the life of the power source is a replacement interval of greater than 12 months or 1000 recognition attempts by a user, whichever comes first.
- The power source must be of a standard size that can easily be obtained.
- The replacement of the power source should be able to be accomplished with no special equipment in less than 20 seconds.
- A low power indicator must be available to indicate that the power source should be replaced.
- At 10 hours after the low power indicator first alerts the need for power source replacement the firearm must be able to fire 3 full magazines.
- The number of steps to test the life of the power source should be minimized.

OPERATION

- The smart gun technology should not require any actions to activate or deactivate.
- The smart gun system must have a method to reinitialize the identifying sequence.
- The system must detect when a new user is attempting to use the firearm.
- The system must detect and disable the firearm when an existing user has relinquished the firearm.

- The smart gun technology must automatically be able to repeatedly enable and disable.
- The smart gun technology must be able to be activated by a single individual without assistance from others.
- The smart gun technology must be able to be operated with one hand.
- The smart gun technology must be able to be operated with either hand.
- The smart gun technology must operate while the user wears gloves made of .063 inch thick leather, or .005 inch thick latex rubber.
- The time for the smart gun technology to attempt to identify the user and enable the firearm must be less than .250 seconds.
- The time for the smart gun technology to attempt to identify the user and disable the firearm must be less than .250 seconds.
- The smart gun technology must not be able to cause the firearm to fire in and of itself.
- The smart gun technology must interface to the firearm in such a manner that the firearm will function if the technology becomes dysfunctional.
- The smart gun technology should only be enabled if the firearm is in an authorized user's hand.
- The smart gun technology should only be enabled if the key is within 6 inches of the discriminator.
- The smart gun technology system should not require the use of a memorized task.
- All users must be enrolled before use.
- The system should allow an untrained user to be enrolled in less than 5 minutes.
- The number of steps to test for an authorized user should be minimized.

KEY

- The key must be unique to an individual or a group.
- The key must be stable and non-changing for a known period of time.
- The key must not be easily copied.
- The key must be controlled in such a manner that no two users would inadvertently have like keys.
- The key should not be transferable, but uniquely associated to a person.
- The key must communicate with the discriminator.
- The key should not be an item that must be separately carried by the individual such as an external device. If an external device must be used it must meet the following requirements.
- An external device must be able to be carried on at least two locations.
- The size of the external device may vary depending on the intended carrying locations.

- The external device must meet same standards as smart gun technology.

DISCRIMINATOR

- The discriminator must be able to identify and differentiate between multiple keys.
- The memory required by the discriminator to store a user's unique characteristic should be minimized.
- The number of different users that should be able to operate a particular firearm should be greater than 50.
- The system should remember enrolled users until un-enrolled.
- The discriminator must be able to activate the latch.
- The false acceptance rate (FAR) should be less than 5%.
- The false rejection rate (FRR) should be 0%.
- The recognition score and the threshold value that is used to determine if a recognition is valid should be available in a test configuration.
- The smart gun technology must be able to perform the identification of the user without regard to the alignment of the key.
- The discriminator must not require special movement for the key to be read.

LATCH

- The latch must be able to lock or unlock the firing state of the firearm.
- The latch should be matched to the characteristics of an individual firearm.
- The latch is activated by the discriminator.
- The implementation of a latching mechanism to lock the firearm for an unauthorized user should not affect the trigger pull level during normal use by the authorized user.
- The material strength of the latch must withstand the stresses of both normal and credible abnormal circumstances.

INDICATORS

- A feedback indicator should be present to show whether the firearm (the latch, not the discriminator) is enabled or disabled.
- Any indication should be obtained with minimal actions from the user.
- Any indicator should not distract the user's attention from their duties.
- Any indicator should not be easily noticed by others.

DOCUMENTATION

- Instructions of proper use must be available.
- The amount of specialized ancillary equipment should be minimized.
- The number of special procedures should be minimized.

SAFETY

- The smart gun technology should not contain material that contains known carcinogens.
- The smart gun technology should not emit known harmful emissions.

OTHER STANDARDS

- The smart gun technology system must meet the existing applicable NIJ standards.
- The smart gun technology system must meet the existing applicable SAMMI standards.

ADVERSARIAL STRENGTH

- The time for an adversary to defeat the smart gun technology system after being taken from an officer should be greater than 1 minute.
- The smart gun technology system should not be defeated with tools readily available.
- An adversary must not be able to overcome the smart gun technology system in a manner that would make the firearm non-functional to the user.

TRAINING

- The training on normal operation of a smart gun technology system should be less than 1 hour.
- Specialized training on smart gun technology system covering topics such as diagnostics and repair should be less than 4 hours.

MAINTENANCE

- The smart gun technology system should be made up of modular parts.
- The smart gun technology system should be tested with normal electrical bench-top equipment.
- Modular parts should have features for easy alignment during assembly, testing, and replacement.
- The smart gun technology system should have diagnostic test signals available.
- The required routine maintenance of the smart gun technology system should require less than 1 hour per year.
- The routine maintenance of a smart gun technology system must be simple enough to be performed by an untrained user.
- Routine maintenance of a smart gun technology system must not degrade the system performance.

INTERFACE

- The mechanical layout of the smart gun technology system should be standardized for potential upgrade capabilities.
- The electrical interface of the smart gun technology system should be standardized for potential upgrade capabilities.

- The information protocol of the smart gun technology system should be standardized for potential upgrade capabilities, and compatibility between different brands of firearms.

COST

- The incremental cost of a smart gun technology system should be less than $60.
- The total cost of maintaining a smart gun technology system should cost less than $5 per year.
- The total miscellaneous cost associated with a smart gun technology system should cost less than $5 per year.

TESTING

- All requirements must be sufficiently tested.
- The smart gun technology system must be trial field tested in actual use conditions.
- The smart gun technology system must be analyzed for failure modes and the effects of failures before fielding the system.

RELIABLILTY

- The smart gun technology system should be able to enable or disable the firearm after identifying the user with a reliability of 99.9%.

SERVICE LIFE

- The lifetime of a smart gun technology must be at least 10,000 live rounds, and 100,000 enable/disable operations.

ENVIRONMENTS

- The smart gun technology system must operate independently of the amount of ambient light.
- The smart gun technology system should operate after submersion in water.
- The smart gun technology system should operate at temperatures up to 160 degrees F.
- The smart gun technology system should operate down to -50 degrees F.
- The smart gun technology system must operate after a drop of 4 feet on to a hard steel plate in any orientation.
- The smart gun technology system should operate after vibration.
- The smart gun technology system should operate after exposure to chemicals commonly used in or around firearms.
- The smart gun technology system must operate during and after acoustical noise environments up to 130 dB.
- The smart gun technology system should operate after exposure to a salt fog environment.
- The smart gun technology system should operate after exposure to sand and dust.
- The smart gun technology system should operate after exposure to mud.

- The smart gun technology system should operate after an exposure to a surf environment.
- The smart gun technology system should operate after ice has been applied and removed.
- The smart gun technology system should operate after exposure to solar energy.
- The smart gun technology system must operate during and after exposure to radio frequency interference.

APPENDIX B

"SMART GUNS" CONSIDERATIONS FOR CIVILIAN APPLICATIONS

Intentionally Left Blank

1.0 INTRODUCTION

As noted in section 1.2 of the main document, the principal focus of this report was the application of "smart gun" technology to the law enforcement officer's primary duty weapon (i.e., the officer's handgun). However, the majority of legislation being considered regarding "smart guns" is focused on the civilian firearms owner. Furthermore, much of the discussion, both for and against, "smart guns" is focused on the civilian applications. As a result, many law enforcement agencies are being asked to review "smart guns" in the context of civilian ownership. NIJ and Sandia chose to include this appendix which is intended to provide some additional information for individuals with this objective.

2.0 SCOPE

This appendix is not a comprehensive review of "smart guns" for civilians. It is outside of the scope of the primary effort. However, in reviewing information for law enforcement applications, one is also exposed to information focused on the civilian application. The information in this appendix is based upon this tangential exposure. Sandia did not test or evaluate any equipment for this effort. Furthermore, Sandia has not formally developed any requirements or evaluation metrics by which to assess the value of "smart guns" to the civilian user. As such, the following paragraphs will provide some thoughts and considerations. However, they should not be construed as full evaluations or providing any metrics based conclusions.

3.0 CIVILIAN USE SCENARIOS FOR "SMART GUNS"

Since Sandia does not have any documented requirements for civilian firearms usage, the scenario approach will again be utilized to provide a framework for the discussion. Three scenarios have been identified. It is likely that there are other uses and scenarios. However, Sandia believes that these three provide a reasonable span of the civilian uses for firearms.

3.1. Scenario 1: Safe Storage of Firearms in the Home

This first scenario is one frequently focused on by proponents of "smart guns". This scenario is one in which a firearm is stored in the home. One of the purposes of owning the firearm may be self defense. For this reason many firearms are currently stored in a loaded and unlocked condition. A "smart gun" would allow a homeowner to have a loaded gun safely stored in the home with reduced risk of accidental discharges by children or guests. It should also prevent an intruder from picking up the weapon and using (firing) it against the unaware homeowner. Even in cases where the weapon is stored unloaded, a "smart gun" would prevent the loading and firing of the weapon unless the person is an authorized user.

3.2. Scenario 2: Sporting use of a Firearm

The second scenario is the use of a "smart gun" in a sporting activity. The most basic use would be plinking or target shooting at a range. This activity would place minimal requirements on "smart gun" technology. Other activities may include competitive shooting. These events may occur in less ideal weather and under more strenuous activity. This comment is especially applicable to activities like International Practical Shooting Confederation (IPSC) competitions. A third variation on the sporting use scenario is the utilization of a firearm while hunting. This

variation introduces potentially even more inclement weather and environmental considerations than even some law enforcement applications. However, in all of these sporting situations, the consequence of a false rejection is not as dire as when a law enforcement officer draws his weapon.

3.3. Scenario 3: Concealed Carry

According to the National Rifle Association's Institute for Legislative Action website (http://www.nraila.org/research/19990729-RighttoCarry-001.html), currently, 44 out of 50 states have some means for law abiding civilians to obtain permits to carry concealed firearms. Of those states, 33 have passed shall issue laws that mandate that permits be issued unless specific cause can be shown justifying denial of the application. Given these figures, there is a significant segment of the civilian population that has a permit or can apply for a permit to legally carry a firearm concealed.

4.0 SCENARIO CONSIDERATIONS

The following paragraphs will discuss some considerations for the feasibility of "smart guns" in the context of these civilian scenarios. It is important when reading these paragraphs to remember that lockable guns currently exist. Some self-locking guns exist and research is ongoing in this area. Personalized "smart guns" do not appear to be likely in the immediate future without several years of research and development. Because of this conclusion regarding personalized "smart guns", this appendix will focus on lockable guns and self-locking guns as they appear to be the categories of "smart gun" most relevant today.

4.1. Scenario 1

Many proponents of "smart guns" advocate them because they believe they will increase the safety in the home. "Smart guns" should reduce gun-related accidents, suicides, and possibly homicides by making it impossible for unauthorized (e.g., children) individuals from discharging the weapon. It is also hypothesized that these weapons may reduce the gun crime and the trafficking in weapons because many of the weapons involved in crimes and gun trafficking are stolen. "Smart guns" are hypothesized to reduce these misuses because they would be less desirable because stolen "smart guns" could not be fired by anyone other than the original authorized user(s).

There are several considerations that are relevant to this scenario. For individuals who currently do not safely store their weapons, it is unlikely that lockable guns will provide much improvement. Either because of a desire to keep the weapon ready or because of a lack of attention or caring they will likely store it unlocked. For these users, a self-locking weapon does provide credible improvement in the storage of the weapon. However, most of the self-locking weapons utilize some type of credential based recognition (e.g., magnetic ring or RF transmitter/receiver combination). These individuals are likely to store the weapon with the credential near the weapon for convenience. This arrangement in most respects negates the increase in safety attributed to the "smart gun". For this type of individual, a biometrics based recognition system on a self-locking firearm would appear to have the greatest value.

For the individuals concerned with the safe storage of their firearms, "smart guns" provide greater benefit. These individuals are likely to take the time to activate lockable guns. Self-locking guns will provide more transparency and will prevent a distracted individual from

forgetting to activate the lock. Credential based recognition systems provide a problem for rapid access, if self defense is a consideration. Assuming these responsible individuals will be unwilling to collocate the credential and the firearm during storage, either the individual must carry the credential at all times or the ability to rapidly activate the weapon is lost. A biometrics based recognition system is vastly superior in this case as well.

Given these observations, it appears reasonable that just as in paragraph 4.2.1.1, of the main document, the rapid-access, lockable storage containers may be preferable to the lockable gun. Furthermore, rapid-access, lockable storage containers may be preferable to credential based, self-locking guns. The user does not have to carry a credential at all times to have rapid access to the weapon and it is more difficult to steal (assuming the hardened container is secured to the floor or other surface). It also prevents unauthorized individuals from even touching the weapon. If rapid access is not a consideration, (i.e., safe storage is the only concern), there are numerous manufacturers of gun vaults and safes in various shapes and sizes that provide even more protection against theft, fire, and unauthorized access. Plus these devices can be used to protect other things besides weapons.

Some of these observations are echoed by the New Jersey Institute of Technology (NJIT) and the Picatinny Arsenal in a "smart gun" study done for the state of New Jersey. As part of their study, NJIT and Picatinny Arsenal reviewed 18 items that had relevance to the "smart gun" discussion. These items ranged from trigger locks to some of the retrofits available for conversion of existing weapons to credential based self-locking guns. None of these items met all of their criteria, but the top three items were locking storage containers.

As to the other claims associated with "smart gun" and home storage, many appear to be speculation. The likelihood of reducing gun thefts and thereby black-market weapons appears to be subject to debate. Part of that debate will depend upon how easily the recognition systems may be bypassed.

As to reducing homicides and suicides in the home, if a weapon is readily available, it is likely to be considered as a tool to commit the murder or suicide.[2] It seems credible to assume that most or all adults in a household would be authorized users or would know how to activate the weapon (i.e., get the credential from storage). It is also highly likely that many children (above some adolescent age) may be authorized or know where the authorization credentials are kept. This statement is made assuming that many households that include guns shoot them at least occasionally. These households are likely to introduce children to the shooting sports and as a result, the children are likely to be authorized to shoot the weapon. If these assumptions prove to be accurate, then the reduction in firearms based homicides and/or suicides due to "smart gun" use is likely to be small. These assumptions may also be another argument for the use of storage containers in that anyone in the family can use a weapon in a supervised situation, but only certain individuals have access to the weapons when they are in storage.

This section is not intended to invalidate the "smart gun" concept or to discourage the research and development of technology in this arena. However, it appears that for the safe storage scenario, locking gun and some self-locking gun implementations will only provide limited improvement.

---

[2] *Number and Distribution of Firearm Injuries and Deaths,* Johns Hopkins Center for Gun Policy and Research, p2, http://support.jhsph.edu/departments/gunpolicy/documents/Factsht.pdf.

4.2. Scenario 2

One area that is not often discussed or discussed only minimally in "smart gun" discussions involves the recreational use of firearms. Guns are used recreationally in many ways. Some, like plinking and target shooting do not impose significant requirements on the "smart gun". It seems reasonable that an occasional false rejection would not adversely impact the recreational shooter. However, frequent false rejections may be annoying enough so as to cause an attempt to bypass the mechanism or obtain a different weapon. Furthermore, some shooters choose to wear gloves either for comfort or protection while shooting during inclement weather. As a result, the environmental reliability requirements and the ability to function with a user wearing gloves apply at some level.

For competitive shooting sports, the cost of a false rejection increases slightly. Many of these competitions are held in the outdoors, so environmental reliability is likely a constraint. Competitive shooters often shoot large amounts of ammunition. These users may stress the longevity and reliability of "smart gun" more than any other civilian user.

Hunting is generally comparable to competitive shooting in consequences of a false rejection. However, there are some dangerous game (e.g., large bears) hunting situations where a false rejection may be life endangering. The inherent nature of hunting indicates that a "smart gun" must be robust, able to function in many different climates and environments, useable with gloves and other limiting clothing.

The needs of scenario 2 seem to lend themselves to the strengths of a lockable gun more than a self-locking gun. Generally speaking, these individuals are familiar with their weapons and practice at least a reasonable amount of time. It is not unreasonable to unlock the firearm during the activity and leave it unlocked, nearly eliminating the possibility of false rejections. However, the gun can still be secured in a remote (i.e., non-home) environment when it is not in use.

4.3. Scenario 3

Scenario 3 is the civilian scenario most like the law enforcement officer scenario. In general, it seems reasonable that the general requirements of the on duty officer carrying a firearm apply to the civilian concealed carry person has well.

In addition, there are additional factors that should be considered. It is difficult to determine which user stands to benefit the most from a "smart gun". The police officer is likely to be the higher profile target. The police officer carries the weapon in an exposed condition making it more visible and more likely the target of a grab. The police officer's job also requires physical interaction/conflict with individuals who are antagonistic. The civilian on the other hand is not a symbolic target as the law enforcement officer may be. The civilian carries the weapon concealed, so it is not a target unless it has been drawn. Generally speaking, civilians do not have to engage in physical confrontations with antagonists as a course of their day to day activities. So, the likelihood of drawing the gun or someone attempting a weapon takeaway appears to be much less for a civilian than a law enforcement officer. Therefore, the benefit of the "smart gun" technology to the law enforcement officer is potentially greater than to a civilian.

However, while some of the people obtaining concealed carry permits will be avid firearms users and extremely familiar with their weapon, many of the permit holders are less familiar with their weapon. In addition, very few civilians will have any training in weapon retention. Most

civilians will not have access to communications, backup officers, defensive tactics training, or alternative weapons such as batons, pepper spray, or another firearm. The civilian may also be less likely to have the mental preparation for a life or death struggle. From this standpoint, it is even credible to consider lesser capabilities, such as some variations of self-locking weapons for the civilian due to the reduced likelihood of an altercation and the likelihood that the civilian will be less capable of handling a violent, physical altercation if it does occur. A "smart gun" may at least reduce the potential injury in the event the civilian is disarmed.

5.0 SUMMARY

Sandia has not done a detailed analysis of "smart gun" requirements or evaluation criteria for civilian application. However, all legislation of which Sandia is aware has focused on the "smart gun" for civilians. Most of the literature and marketing activity is at least in part focused on the civilian application of "smart guns". As a result, NIJ and Sandia chose to include this appendix.

Based upon Sandia's observations, it appears reasonable to represent the majority of civilian firearms uses by three scenarios:

- Scenario 1: Safe storage of a firearm in the home.
- Scenario 2: Recreational use to include plinking, informal target shooting, competitive shooting, and hunting.
- Scenario 3: Concealed carry by an authorized civilian

The effectiveness is Scenario 1 of "smart guns" seems to be very dependent upon the responsibility of the user and the category of "smart gun". It also seems that for many responsible gun owners, a quality locking container may provide comparable benefits to lockable and self-locking guns. Lockable guns appear to have some strong benefits for Scenario 2 situations. Self-locking guns could be equally valuable, but the possibility of false rejections is likely to be greater for no added benefit. Scenario 3 situations are very similar to law enforcement applications. The law enforcement officer is a more likely, higher profile target, but also has training and alternatives that the civilian does not. So, it is possible that the civilian user may be able to benefit more from "smart gun" technology. The benefit to civilians may even be there for self-locking guns, which in general do not meet the needs of the law enforcement officer.

Intentionally Left Blank

DISTRIBUTION

50	MS	National Institute of Justice Attention: Wendy Howe Room 7233 810 7th Street NW Washington, DC 20531
100		National Law Enforcement & Corrections Technology Center C/O Lance Miller 2277 Research Boulevard/MS-8J Rockville, MD. 20850
3	MS	0759 J. W. Wirsbinski, 5845
3		0775 G. Smith, 5861
1		0783 J. Lavasek, 5854
1		0888 D. A. Loy, 6245
1		1050 W. J. Suderman, 3124
1		1131 D. L. Buie
1		1425 K. B. Pfeifer, 1744
1		9018 Central Technical Files, 8945-1
2		0899 Technical Library, 9616
1		0612 Review & Approval Desk, 9612