**U.S. Department of Justice**
Office of Justice Programs
*National Institute of Justice*

JUNE 2013

NATIONAL INSTITUTE OF JUSTICE

# RESEARCH REPORT

# A Review of Gun Safety Technologies

BY MARK GREENE, Ph.D.

NIJ

U.S. Department of Justice
Office of Justice Programs

810 Seventh St. N.W.
Washington, DC 20531

**Eric H. Holder, Jr.**
Attorney General

**Karol V. Mason**
Assistant Attorney General

**Greg Ridgeway**
Acting Director, National Institute of Justice

This and other publications and products of the National Institute of Justice can be found at:

**National Institute of Justice**
http://www.nij.gov

**Office of Justice Programs**
Innovation • Partnerships • Safer Neighborhoods
http://www.ojp.usdoj.gov

JUNE 2013

NATIONAL INSTITUTE OF JUSTICE

RESEARCH REPORT

# A Review of Gun Safety Technologies

BY MARK GREENE, Ph.D.

NCJ 242500

NIJ

## Highlights

- Since the mid-1990s, numerous teams have developed firearms with advanced gun safety technology—often called "smart guns" or "personalized firearms"—to varying degrees of technological maturity.
- These firearms are designed to contain authorization systems which generally combine an authentication mechanism that actuates a blocking mechanism in a seamless process that is designed to take less time than handling and firing a conventional gun.
- At least three products—two handguns and a shotgun—have been developed in the private sector by Armatix GmbH, Kodiak Industries, and iGun Technology Corporation that could at least be described as *commercializable* or *pre-production*.
- There are no personalized firearms available commercially in the United States yet today, but Armatix and Kodiak are planning to bring their respective products to market in 2013.
- Armatix of Germany has developed the Smart System which is composed of a .22 caliber pistol called the iP1 that is activated by the iW1, a device worn on the wrist like a watch that communicates using radio frequency identification (RFID).
- Armatix reports that it has sold the Smart System in Europe and Asia and is pursuing approval for commercial sale in the United States through its U.S. subsidiary Armatix USA.
- Kodiak Industries of Utah recently launched the Intelligun, a fingerprint-based locking system installed on a model 1911-style .45 caliber pistol that is available for pre-order from Kodiak with a projected delivery date later in 2013.
- The Intelligun system will add an equivalent weight of less than one round to the total weight of the firearm and is reported to have an expected failure rate of 1 in 10,000, which is reported to be less than the expected failure rate of the firearm it is installed on.

- iGun Technology Corporation of Florida developed in 1998 the M-2000, a shotgun that could be considered the first personalized firearm where the user wears a ring with a passive RFID tag embedded that communicates with an RFID reader onboard the firearm.
- iGun performed a number of tests and determined that the unit was reliable and estimates that enough components were created in 1998 to assemble 50 working units, but the project was shelved due to market research showing limited consumer demand.
- The reliability of smart guns remains a topic of interest since early efforts at development in the mid-1990s, with *reliability* indicated as the most important concern by law enforcement practitioners regarding the potential use of this technology in a report published in 1996 that was funded by the National Institute of Justice.
- Reliability can be defined as the probability that a device will perform its intended function for a specified period of time under stated conditions.
- Test protocols already promulgated by U.S. Government agencies and other standards organizations, or protocols that could be developed, could be used to test engineered firearm systems under different operating conditions to provide quantitative metrics on reliability.

## Table of Contents


About the Report 7
Developing the Report 9
Acknowledgments 12
Executive Summary 13
A Perspective on Risk, Reliability, and Person-centric Technologies 19
Technologies for User Authorization 24
- Token-Based Technologies 24
- Biometric Technologies 26

Technology Readiness Levels 27
Technology Quick Reference Tables 29
- Upper Tier 29
- Middle Tier 30
- Lower Tier 33

Technology Developers 34
- Sandia National Laboratories 34
- Colt's Manufacturing Company, Inc. 36
- iGun Technology Corporation 39
- Smith & Wesson 43
- FN Manufacturing, Inc. 45
- New Jersey Institute of Technology 50
- Metal Storm 54
- University of Twente 57
- Armatix GmbH 57
- Safe Gun Technology 65
- TriggerSmart 67
- Kodiak Industries 69
- Biomac Systems, Inc. 75

Online Resources 77
Glossary of Acronyms Used 79
References 82

# A Review of Gun Safety Technologies

**BY MARK GREENE, Ph.D.**

## About the Report

When such an issue with deep and powerful cultural resonance as firearms is given the full attention of the nation, the challenges involved with confronting the complex interconnectedness of law, public safety, Constitutional rights, policy, technology, market forces, and other concerns seem only amplified. With careful consideration, however, untangling the various components of the issue is possible, and an investigation of technology can be accomplished with minimal diversion into the other realms.

This report examines existing and emerging gun safety technologies and their availability and use to provide a comprehensive perspective on firearms with integrated advanced safety technologies. These firearms are known by various terms such as smart guns, user-authorized handguns, childproof guns, and personalized firearms. A "personalized firearm" can be understood to utilize integrated components that exclusively permit an *authorized user* or set of users to operate or fire the gun and automatically *deactivate* it under a set of specific circumstances, reducing the chances of accidental or purposeful use by an *unauthorized user*.

A report published in 2005 entitled *Technological Options for User-Authorized Handguns: A Technology-Readiness Assessment* discussed this in the context of two defined types of handgun 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).[1] The National Academy of Engineering (NAE) Committee on User-Authorized Handguns published this report seeking to clarify the technical challenges of developing a reliable user-authorized handgun (UAHG) to reduce certain types of handgun misuse.

The goal of this work is to provide an objective, neutral perspective on existing and emerging gun safety technologies and their availability and use today. In assessing what technologies and products exist or may exist in the near future, it is important to clarify what the technologies can and cannot do, to distinguish the difference between fact and fiction, and to manage expectations about how these firearms could reasonably be expected to perform. The material presented here should be considered in a sober manner with the understanding that the use or misuse of any firearm regardless of what technology may or may not be integrated could lead to injury or death.

Any information presented here shall not be construed to be an endorsement of any particular technology, developer, patent, company, or approach. Furthermore, any information that may not be included here shall not be construed as disapproval. Finally, given the various perspectives and opinions on firearms, any topic discussed here with a nexus to technology that may also overlap with another dimension of the greater national conversation about firearms shall not be construed to be a substantive discussion of the topic outside of the technologically focused perspective presented here.

## Developing the Report

The National Institute of Justice (NIJ) was tasked with supporting the President's Plan to Reduce Gun Violence,[2] specifically:

*"The President is directing the Attorney General to work with technology experts to review existing and emerging gun safety technologies, and to issue a report on the availability and use of those technologies."*

In support of this Executive action, NIJ has conducted a technology assessment and market survey of existing and emerging gun safety technologies that would be of interest to the law enforcement and criminal justice communities and others with an interest in gun safety. This assessment builds on previous technology reviews on this topic area produced by Sandia National Laboratories in 1996[3] and 2001[4] and the National Academy of Engineering in 2003[5] and 2005.[6] The assessment examines *smart* or *personalized* technologies implemented into firearms that prevent anyone other than an authorized user from firing it. Example gun safety technologies include proximity devices, such as radio frequency identification (RFID) chips and magnetic rings, and biometric devices, such as fingerprint scanners. The assessment also examines firearms that employ electronic or software components integrated into safety mechanisms. The report summarizes past and present research and development (R&D) and product development efforts in industry, academia, and government. It includes a technical assessment of each development effort and contains an estimation of technology maturity for each effort reviewed.

The assessment was led by a General Engineer in the Office of Science and Technology at NIJ with assistance from technical staff at the Sensor, Surveillance, and Biometric Technologies Center of Excellence (hereafter cited in the text as the "SSBT Center"). The SSBT Center is operated by ManTech International Corporation under NIJ award 2010-IJ-CX-K024 and is a Center within the National Law Enforcement and Corrections Technology Center (NLECTC) System funded by NIJ. The SSBT Center

provides scientific and technical support to NIJ's sensor, surveillance, and biometrics R&D efforts as well as technology assistance, information, and support to criminal justice agencies. The primary role of the Centers of Excellence is to support NIJ's research programs in different technical areas and to assist in the transition of law enforcement technology from the laboratory into practice by first adopters. They assist NIJ in identifying the technology needs of the criminal justice community and conduct related research, test, and evaluation activities. The Centers of Excellence are the authoritative resource within the NLECTC System for both practitioners and developers in their technology area(s) of focus.

To assist with information gathering of technology and technology-related issues to inform this report, NIJ organized a workshop on gun safety technologies in March 2013. Representatives from a majority of the entities covered in this report were present to have the opportunity to discuss their technology, R&D efforts, product development, and technology-related issues. Relevant staff from the Department of Justice, Department of Homeland Security, Department of Defense, and the Office of Science and Technology Policy attended as well as participants from several outside organizations including firearms manufacturers, the Sporting Arms and Ammunition Manufacturers' Institute (SAAMI), and the Johns Hopkins Center for Gun Policy and Research. Discussion topics included modern history of gun safety technology and early R&D in smart guns (ca. 1994–2006); existing and emerging gun safety technology and smart guns today (ca. 2006–present); availability and use of gun safety technology and smart guns today, including a broad discussion of potential users and user requirements; technological barriers to developing reliable and effective technologies and products; and market barriers to introducing reliable and effective technologies and products.

In support of research activities, NIJ and the SSBT Center pursued several sources of information from February to May 2013: site visits, face-to-face meetings, telephone interviews, technology demonstrations, email correspondence, literature review, online investigations, NIJ archival documents, and Bureau of Justice Assistance (BJA) archival documents.

SSBT Center staff visited the following organizations in March and April of 2013:

- Kodiak Industries
- iGun Technology Corporation
- New Jersey Institute of Technology
- University of Massachusetts Lowell
- Safe Gun Technology
- Armatix GmbH
- TriggerSmart

The following organizations declined individual interviews or meetings for this report, which may not have been due to a lack of interest but rather a lack of an ongoing program in this topic area. However, they were responsive to email correspondence and telephone calls:

- Colt Defense
- Colt's Manufacturing Company LLC
- FN Manufacturing
- FN USA
- Metal Storm
- Smith & Wesson
- Sturm, Ruger & Co.

Each entity listed in the Technology Developers section, except for Sandia National Laboratories, was afforded the opportunity to review a draft version of the following report content: the Technology Readiness Levels section, the general portion of the Technology Quick Reference Tables section, their specific table, the brief general portion of the Technology Developers section, and their specific subsection from the Technology Developers section. The content on Sandia National Laboratories is drawn from published reports that are publicly available, so no further review from Sandia was sought in that particular case. The report as a whole was reviewed by personnel at the Department of Justice, Department of Homeland Security, and Department of Defense with knowledge or experience with firearm technology or smart gun R&D.

NIJ also released a Federal Register notice on February 20, 2013, to alert the public that NIJ was conducting this review.[7] This public notice encouraged stakeholders to self-identify and provided accessible means to relay relevant information and comments to NIJ through an online resource hosted on the NLECTC website (www.justnet.org) or a dedicated email address established for this effort (gunsafetytechnology@usdoj.gov). No comments were received from the public that were found to be responsive to the needs of the report.

The assessment did *not* include any research into legislature, social, or community policy or politics; did *not* cover integration of gun safety technologies into law enforcement procedures in the field (e.g., police patrol duties); and did *not* include physical testing of identified devices or products. However, the report will discuss documented critical requirements of the gun owner or user in order to properly enable smart gun technology.[8,9] The objective of the assessment is ultimately to provide an unbiased summary of existing and emerging technologies and the availability and use of those technologies to inform any future Federal R&D strategy and innovation in gun safety technology across the community of practice and technology ecosystem.

## Acknowledgments

The National Institute of Justice would like to acknowledge personnel from the following organizations for providing information regarding their technology, products, intellectual property, and other activities related to gun safety technology (in alphabetical order): Armatix GmbH, Armatix USA, Biomac Systems, iGun Technology Corporation, Kodiak Industries, New Jersey Institute of Technology, Safe Gun Technology, TriggerSmart, and the University of Twente. NIJ would like to thank personnel at the NLECTC National Center for photographs of the Sandia demonstrators and one of the Colt prototypes. NIJ would also like to acknowledge personnel from the Firearms Technology Branch, Bureau of Alcohol, Tobacco, Firearms and Explosives; the Department of Homeland Security, Science and Technology Directorate; and the U.S. Army Armament Research, Development and Engineering Center for reviewing the draft manuscript of this report.

## Executive Summary

Since the mid-1990s, numerous teams were found to have developed firearms with advanced gun safety technology to varying degrees of maturity. These firearms, often called smart guns or personalized firearms, are designed to contain authorization systems which generally combine an authentication mechanism that actuates a blocking mechanism in a seamless process that is designed to take less time than handling and firing a conventional gun. At least three products—two handguns and a shotgun—have been developed by innovators in the private sector that are at a technological maturity level that could at least be described as *commercializable* or *pre-production*. The innovators are Armatix GmbH, Kodiak Industries, and iGun Technology Corporation. There are no personalized firearms available commercially in the United States yet today, but Armatix and Kodiak are planning to bring their respective products to market in 2013.

Armatix of Germany has developed the Smart System which is composed of two main parts, the iP1 and the iW1. The iP1 is a .22 caliber pistol that is activated by the iW1, a device worn on the wrist like a watch that communicates using radio frequency identification. Armatix reports that it has sold the Smart System in Europe and Asia and is pursuing approval for commercial sale in the United States through its U.S. subsidiary Armatix USA. It has submitted the Smart System for testing in laboratories for certification by relevant Federal and state authorities and organizations.

Kodiak Industries of Utah developed the Intelligun, a fingerprint-based locking system installed on a model 1911-style .45 caliber pistol to unlock the firearm for operation immediately for authorized users. The Intelligun system will add an equivalent weight of less than one round to the total weight of the firearm and is reported to have an expected failure rate of 1 in 10,000, which is reported to be less than the expected failure rate of the firearm it is installed on. Kodiak launched the Intelligun in 2012 and debuted it in 2013 at a widely attended annual firearms

trade show. A 1911-style pistol with the Intelligun system installed is available for pre-order from Kodiak with a projected delivery date later in 2013.

iGun Technology Corporation of Florida developed in 1998 the M-2000, a shotgun that could be considered the first personalized firearm to go beyond a prototype to an actual commercializable or production-ready product. The M-2000 operator wears a ring with a passive RFID tag embedded that transmits a specific code when energized by the RFID reader onboard the shotgun. iGun performed a number of tests and determined that the unit was reliable. iGun shelved the project due to market research showing limited consumer demand but estimates that enough components were created in 1998 to assemble 50 working units.

NIJ funded over $11.1M in research and development projects over more than a decade from the mid-1990s through the mid-2000s to investigate different technologies and develop functional prototypes of handguns with electronic safety mechanisms built in that would prevent anyone other than an authorized user from firing it. NIJ supported requirements gathering and technology reviews in this topic area, which were published by Sandia National Laboratories in 1996[10] and 2001.[11] Various scenarios such as law enforcement firearms being seized in the field and used against officers, accident prevention in the home, child safety, and preventing the use of stolen firearms in criminal activities were considered as possible use cases where smart guns could have an impact. In addition, from 2008 to the present, the Bureau of Justice Assistance has also provided just over $1.5M to fund a project begun through NIJ. NIJ also participated in workshop and review efforts by the National Academy of Engineering in 2003[12] and 2005.[13]

In total, the Office of Justice Programs (OJP) has supported at least $12.6M in gun safety technology research over the past fifteen years that has catalyzed the development of some early experimental designs that have incorporated a range of technologies that have helped build a foundation upon which subsequent efforts have followed. The history

of research and development in smart guns has shown this to be a challenging technology area, and a number of well-known names from the firearms industry have pursued serious efforts to produce functional prototypes over the years. While none were successful enough with their designs to bring models to the marketplace, the initial R&D has provided a wealth of knowledge and experience on which to build.

In 1997, NIJ awarded $500,079 to Colt's Manufacturing Company, Inc. of Hartford, CT, to develop a smart gun based on an earlier design it developed independently based on radio frequency communication. The Colt device had a wristband that communicated with the firearm which enabled a mechanical actuator in the handgun when in close proximity. In March 2000, two prototypes demonstrated that it was possible to integrate its concept into a handgun; however, the prototypes proved unreliable and not ruggedized enough to permit serious test firing, so reliability evaluations could not be conducted. Although Colt evidently also funded R&D internally to move its technology forward, it curtailed further efforts in this area around this time.

Between 2000 and 2005, NIJ provided $3,673,361 to Smith & Wesson of Springfield, MA, to develop a handgun that could only be used by an authorized user. Smith & Wesson explored different methods of authentication including PIN codes, biometric fingerprints, and skin tissue spectroscopy approaches. Prior to the cooperative agreements with NIJ, Smith & Wesson reported it had internally funded a grip sensor that was incorporated in the handle of the handgun. Although Smith & Wesson proposed a goal of delivering 50 prototypes for test and evaluation, reliably integrating the electronics into the firearm proved to be a challenge and ultimately only two demonstration items were delivered.

Between 2000 and 2006, NIJ provided $2,606,156 to FN Manufacturing, Inc., of Columbia, SC, a subsidiary of FN Herstal, to develop an RFID-enabled handgun called the Secure Weapon System (SWS). FN provided a comprehensive technical report on the SWS and a designed, developed, and integrated prototype that represented the combination of selected

specifications. The demonstration item used a ring worn on the finger that contained an RFID tag embedded in it and a piezoelectric mechanism built into the handgun to prevent the firearm from firing when the ring was out of proximity. Three prototypes fired a combined 1,500 rounds with only one mechanical incident that was resolved, although erratic behavior was also observed in the authorization system and blunt mechanical force could override the electromechanically controlled blocking pin which would allow the gun to fire by an unauthorized user. In the absence of additional funding for more research and testing, the project was not pursued further.

In 2002, NIJ awarded over $1.1M in a number of smaller awards to various performers who were exploring different technologies that could be used for automated authentication of a firearm user. Among these awards, iGun Technology Corporation, which developed the M-2000 shotgun, partnered with West Virginia University to produce a report on the use of biometric modalities and the potential integration of appropriate technologies into a handgun for law enforcement. Prior to this, iGun had privately developed a working shotgun by 1999 with an internal safety mechanism that can be unlocked with a passive RFID tag embedded in a ring worn by the user that is preprogrammed with unique authorized identification codes. Another awardee in this group was Metal Storm, an Australian company, which investigated the development of a handgun that was fired entirely electronically. The concept gun also had multiple barrels that could accommodate less lethal rounds such as small beanbags.

Between 2004 and 2008, NIJ provided $2,515,475 to the New Jersey Institute of Technology (NJIT) to develop and demonstrate a technology for firearm user authentication based on dynamic grip recognition. The design of its Child Safe Personalized Weapon uses multiple pressure sensors located on the left and right grip pads of the gun located on the handle. NJIT has focused on using existing popular models of pistols as a platform to develop its technology and attempted to cultivate a relationship with Taurus, a manufacturer of handguns, at the early stages of the project, but used Beretta as its platform instead. From 2008 to the present, BJA has provided $1,504,818 to NJIT to further develop its technology.

Other developers of smart guns include TriggerSmart, a startup based in Ireland partnered with the Georgia Institute of Technology, which reports prototype firearms also based on RFID technology. The firearm portion of the TriggerSmart system will be a user replacement part. For example, to convert a rifle to the TriggerSmart system, the user would replace the factory installed lower receiver with a lower receiver designed by TriggerSmart. It has built three demonstration firearms—a handgun, a rifle, and a shotgun—and reports that it has successfully fired the guns over 1,000 times. The technology has not been tested beyond the prototype stage, nor has it been tested by a third party; however, the technology has been integrated into reasonably realistic demonstration models.

Safe Gun Technology (SGT), based in Columbus, GA, has developed a prototype user-authorized version of a Remington 870 shotgun with an authorization system that utilizes a fingerprint identification sensor module. The SGT system utilizes an "authorize once" step to arm the gun, which remains in an armed status as long as a hand applies pressure to a grip. If pressure is released on the grip or the gun dropped for longer than one second, the system de-authorizes. No finger is necessary on the scanner after initial authorization, provided pressure to the grip is maintained. Although current design plans are focused on law enforcement, this technology could be used by the general public.

An acknowledgement of firearms as unique among commercial products is warranted. The reliability of smart guns has been a topic of discussion since early efforts at development in the mid-1990s. In the 1996 report published by Sandia National Laboratories and funded by NIJ, *reliability* was indicated as the most important concern by law enforcement practitioners regarding the potential use of this technology. This research was focused on the problem of police firearm takeaways by adversaries and how the use of technology could prevent officers' injury or death due to their own or another officer's firearm being used against them. From all the concerns that were categorized from a survey of law enforcement, a list of user requirements was generated that featured reliability at the top of the list.

That requirement was stated as, "*The addition of a smart gun technology must not significantly reduce the reliability of the firearm system compared to existing firearms*."[14]

Reliability can be defined as the probability that a device will perform its intended function for a specified period of time under stated conditions.[15] Pulling the trigger to make the gun fire is the intended function of the product. Safety features in general, by their very nature, are intended to mitigate the risks associated with the use or misuse of a product. Test protocols already promulgated by U.S. Government agencies and other standards organizations, or protocols that could be developed, could be used to test engineered firearm systems under different operating conditions to provide quantitative metrics on reliability. These measurements could also provide some insight into how human factors relate to the outcomes by repeating them under different stated conditions. Where person-centric technologies associated with the authorization systems may introduce variation in performance among product users, including the human operator in the analysis may help distinguish reliability from related concepts such as usability, durability, maintainability, and proficiency.

## A Perspective on Risk, Reliability, and Person-Centric Technologies

Before proceeding with a discussion of the technology, an acknowledgment of firearms as unique among commercial products is warranted. Pulling the trigger to make the gun fire is the *intended function* of the product. Safety features in general, by their very nature, are intended to mitigate the *risks* associated with the use or misuse of a product, and so unintended injury or death due to accidental discharge, mishandling or misuse by an untrained or unauthorized individual such as a child, and other domestic tragedies are examples of incidents that advanced safety features might effectively address.[16] Preventing the operation of an illegally possessed firearm for criminal purposes or against law enforcement—or outright deterring illegal acquisition of a firearm in the first place—are benefits that may also be addressed by advanced safety features.

Despite these potential benefits, the reliability of firearms with integrated advanced safety technologies has been cited as a concern regarding the potential performance and user acceptance of products that may incorporate such technologies.[17] The underlying concerns about reliability could be anecdotally expressed in many ways, but can generally be described as skepticism of the technology due to a fear that such technology will cause the firearm to malfunction during a situation at the critical instant when a life-or-death decision has to be made. It is understandable that the existential weight associated with any hypothetical scenario involving the use of a firearm in the line of duty or in defense of oneself, family, or home could trigger such visceral concerns. Certainly, no safety feature will ever completely eliminate negative consequences due to human factors, malfunction, or criminal activity. The risks potentially attenuated by integrating safety technology may be weighed against any change in risks associated with the reliability of incumbent products

versus similar alternatives with safety features when both are operated for their intended use. Both reliability *and* risk are therefore integral to the discussion of such person-centric safety technologies, as they can shape both the development of products and the perceptions about them.

The origin of reliability as a technical issue with respect to smart guns can be traced back to at least the mid-1990s. In a 1996 report published by Sandia National Laboratories and funded by NIJ, *reliability* was indicated as the most important concern by law enforcement practitioners who responded to a survey distributed by the researchers.[18] This research was focused on the problem of police firearm takeaways by adversaries and how the use of technology could prevent officer injury or death due to their own or another officer's firearm being used against them. Over 300 surveys were received from respondents with different levels of law enforcement experience and differing responsibilities within their organizations. The questionnaire contained several closed-ended questions that asked about various items and issues related to smart guns and utilized a familiar Likert scale for responses ranging from strongly disagree to strongly agree. It also contained two open-ended questions that asked practitioners to list their two main concerns about a smart gun and two ways a smart gun could cause them problems. The open-ended questions were used to capture the attitudes and opinions of the respondents in their own words, whereas the closed-ended questions were used to measure attitude intensity. To reduce the variety of answers, the open-ended responses were interpreted into several qualitative categories such as reliability, cost, and acceptance by officers. The number of concerns that were categorized as related to reliability was almost three times that of any other category, and many of the other categories had hints of reliability in them as well.

From all the concerns that were categorized, a list of user requirements was generated that featured reliability at the top of the list. That requirement was stated:

"*The addition of a smart gun technology must not significantly reduce the reliability of the firearm system compared to existing firearms*."[19]

Reliability here is defined in relative terms, and so a basis for test and evaluation of reliability must be established which can provide this comparative measure. In *The Assurance Sciences: An Introduction to Quality Control and Reliability*, Halpern discusses how reliability can be a subjective expression of user expectations but it may assume a more definitive character such that it can be defined, computed, tested, and verified.[20] It is not known whether a methodology has ever been applied to provide the comparison suggested in this requirement in a rigorous and scientific way.

The United States Army, for example, uses a Test Operations Procedure (TOP) to determine the reliability of its firearms for its operators.[21] This TOP provides procedures for testing small arms, which includes hand and shoulder weapons and machine guns, including crew-served weapons and light automatic cannons up to 50 millimeters in caliber. While some of the equipment mentioned is restricted for military use only, the TOP is generally applicable to firearms defined under 27 CFR 478.11 that are legal to possess in the United States or reasonably could be adjudicated legal to possess. A discussion of test protocols is beyond the scope of this report, although it is worth noting that a test procedure such as this could provide a framework that may contain all the elements necessary to evaluate any firearm *with or without* integrated advanced safety technologies that might be relevant to the law enforcement or commercial markets. For example, this TOP indicates that, to test the reliability of handguns, at least 6,000 rounds are to be fired and all instances of malfunctions and failures recorded. Other tests expose the firearms to adverse conditions—such as extreme temperatures, rain, sand, and dust—and rough handling such as 1.5 m (5 ft) drops in different orientations. Test procedures promulgated by other relevant technical organizations and standards may also be applicable.[22]

While the concerns collected by the Sandia researchers were constructively converted into user requirements for technology, they should not be confused with a critique of the extant smart gun technology of the mid-1990s since there was essentially nothing available to assess. The user

requirements were translated into a set of engineering requirements, or specifications, which were used as criteria for future R&D and to help design demonstrators to illustrate the various user authorization technologies. As outlined later in this report, various research and development teams within the technology ecosystem at both firearms manufacturers and academic institutions developed prototypes based on similar criteria to what was outlined in the Sandia report using funding from NIJ and other sources. While most demonstrations of smart gun *prototypes* developed in the 1990s and 2000s failed to reach a threshold of performance to meet the defined requirement above, many of the designs reached an estimated level of technological maturity in the range between a proof-of-concept and operational testing.[23]

Perceptions regarding gun safety technology based on *prototype performance*, however, could stimulate misconceptions about how finished *commercial products* might perform, which should be judged on their own merit. There has not yet been a firearm with integrated gun safety technology available commercially, at least not in the United States, and it is only recently that viable product designs have reached a *commercializable* or *production-ready* level of maturity. An exception to this observation is one model of firearm with integrated gun safety technology developed in 1998–1999 that was reported by the inventor to be as reliable as incumbent products based on a number of standardized tests conducted around 2000.[24] It was reported to be at a technological readiness level that would have made it a candidate for the marketplace, although commercialization was not pursued for business reasons, cited as a perceived lack of demand.[25] Whether that previous market research holds today is unknown or what the market demand by consumers would be if commercial products were shown to be reliable. No data has ever been collected and made publicly available for analysis that has demonstrated the overall system reliability of these kinds of firearms. And would acceptance of the technology by law enforcement make a difference to consumers?

The risks that may be associated with the reliability of the firearm are related to the probability that the firearm will fail to perform its *intended*

*function*. Pulling the trigger to make the gun fire is the intended function of the product. Since reliability can be defined as *the probability that a device will perform its intended function for a specified period of time under stated conditions*,[26] this can be measured by the number of times the firearm operates correctly when the trigger is pulled. Alternatively, this could be expressed as a failure rate. However, the firearm is an engineered system and must take into account all the various components—the firing mechanisms, ammunition, safety mechanisms, and other components—when considering failure modes. Within this context are four separate functional results:

1. the gun fires when the trigger is pulled and that is the desired result (true positive);
2. the gun fires when the trigger is pulled and that is not the desired result (false positive);
3. the gun does not fire when the trigger is pulled and that is the desired result (true negative); and
4. the gun does not fire when the trigger is pulled and that is not the desired result (false negative).

This four-state functional result framework is generic enough to hold for *any* kind of firearm with any kind of safety mechanism regardless of whether it involves integrated advanced safety technology or not. A receiver-operator characteristic (ROC) graph[27] or a detection error tradeoff (DET) graph[28] could be constructed using a test methodology common to firearms of a similar type (e.g., pistol) to compare the differences in performance among various devices or products from which reliability can be measured.

These measurements could also provide some insight into how human factors relate to the outcomes by repeating them under different *stated conditions* (e.g., different circumstances or scenarios with different operators). For example, the performance when a firearm is being used by someone not under duress in the absence of any external stress, like at target practice at a range, could be compared to the performance

of firearm use under duress for both conventional guns and guns with integrated advanced safety technologies. Where person-centric technologies may introduce variation in performance among product users, including the human operator in the analysis may help distinguish reliability from related concepts such as usability, durability, maintainability, and proficiency. The risks that may be associated with a firearm to properly deliver a *desired outcome* versus an alternate outcome in a confrontational scenario, for example, may go beyond the measured reliability.

## Technologies for User Authorization

Technologies that are outlined here have been integrated into the various firearms described in this report to enable authorization of the user. An authorization system generally combines an authentication mechanism which actuates a blocking mechanism in a seamless process designed to take less time than handling and firing a conventional gun. The authentication mechanisms use radio frequency identification, biometrics such as fingerprints, or some other technology that can be used to establish a unique identity. This unique identity in general is not required to be something intrinsic to a user, such as a fingerprint, but could be a unique code broadcast at very short distances by an RFID token worn as a ring or watch by the operator. Once a user is identified and authenticated, authorization systems will typically energize an electronic circuit that produces a physical change such as removing a mechanical block to allow the gun to fire. Blocking mechanisms that have been employed include solenoids, motors, and piezoelectric devices which can be used as actuators that respond to signals from the authentication mechanism.

**Token-Based Technologies.** Token-based technologies require the use of an additional physical item—such as a ring, watch, card, or bracelet—to allow for the operation of the system. These tokens may be carried by, worn by, or even implanted into an authorized user. In general, an external token requires that the user remember to have it on their person and is susceptible to theft by unauthorized individuals. Stolen token devices can then be used to authorize their associated firearm. However, additional

security measures built into the token device, such as a token device with a personal identification number (PIN) code, may mitigate use by unintended users.

*Radio Frequency Identification (RFID) Technologies.*[29] RFID is the wireless use of radio frequency electromagnetic fields to transfer data for the purposes of automatically identifying and tracking tags attached to objects. Some tags require no battery and are powered at short ranges by electromagnetic induction. These are called passive tags. Others use a local power source and emit radio waves. These are called active tags. The tag contains electronically stored information which may be read from up to several meters away. Unlike a bar code, the tag does not need to be within line of sight of the reader and may be embedded in the tracked object.

In the context of this report, RFID-based token technologies establish a communication channel between the firearm and the token. Typically, the RFID reader on the firearm broadcasts a signal looking for a token, then a coded signal is sent from the token to the firearm which will authorize the gun to be fired. This technology works while wearing gloves and can be implanted subdermally, as was recommended in the 2005 NAE report.[30] It should be noted that any RF technology could be impacted by interference, but it would depend on a number of factors such as operating frequency and operating range. Uses at the ranges described here are less susceptible to interference due to the very short operating distances.

*Ultrasonic Technologies.* In the one case of an ultrasonic based token,[31] the token is worn on the body of the user and emits an ultrasonic coded signal that is received by the firearm or vice versa. The frequency of the sound is too high for humans to hear, and can be used for determining proximity of the gun. If the gun is not within a specified range, it automatically deactivates. This technological approach has not been widely adopted.

*Magnetic Technologies.* In the one case of a magnetic token,[32] a permanent magnet is simply used to magnetically move a blocking mechanism located in the interior of the firearm. This technological approach has not been widely adopted.

**Biometric Technologies.**[33] Biometric technologies utilize unique features of individuals as the "key" to identify authorized users. Some examples of biometric technologies include fingerprint, palm print, voice, face, and vein pattern, although not all of these are used for firearm authorization. Appropriate electronic sensors or readers are used to collect the biometric and compare it to those of authorized users stored in computer memory.

*Fingerprint Technologies.* To initiate authorization, the user places their finger on a fingerprint sensor. The reader is typically placed in an area that is easily and normally accessible with little or no conscious effort by the user, such as on the grip of where the finger normally rests. Once the fingerprint is scanned, it is quickly compared to an internally stored list of fingerprints of authorized users. If a match is found, the firearm is enabled; otherwise, it remains in the locked state.

*Palm Print Technologies.* Palm print technologies work like fingerprint technologies and use the palm print as the unique identifier. No evidence was uncovered in compiling this report that demonstrates that palm print technology has ever been successfully integrated into a firearm authorization system.

*Dynamic Grip Technologies.* Dynamic grip recognition (DGR) is an emerging biometric authentication method based on the human grasping behavior. A dynamic biometric is a combination of physical and behavioral characteristics that is measured over a duration of time versus a point in time. It is not based on an inherent physical trait of an individual, such as a fingerprint, but rather that grasping behaviors can be used as an identifiable activity. Examples of attributes that could be measured as part of DGR include hand size, hand geometry, and the pressure or strength a hand places on an item at various points. Research on DGR remains

ongoing and no evidence was uncovered to suggest that this approach has been validated or widely accepted yet by the biometrics community of practice.

*Static Grip Technologies.* Static grip recognition (SGR) is an emerging biometric authentication method based on the human grasping behavior at a fixed moment in time. It is similar to DGR, described above, but does not involve measurements of user action or data over time. Instead SGR simply measures the pressure applied by holding the firearm. Research on SGR remains ongoing and no evidence was uncovered to suggest that this approach has been validated or widely accepted yet by the biometrics community of practice.

*Optical Technologies.* Authorization techniques that utilize optical methods for identification may rely on spectroscopic data, such as slight variances in skin color, or image data, such as vein pattern recognition in the palm of the hand. These typically operate in the visible or near-infrared regions. Previously collected optical data of a certified user would be compared to the data collected from a potential user to decide whether to authorize the user. This technological approach has not been widely adopted.

## Technology Readiness Levels

The Department of Defense publishes a guide to assess the maturity of technologies as they evolve through the research, development, test, and evaluation process.[34] There are nine Technology Readiness Levels (TRL) used to describe a technology from the observation of basic principles on which a technology is built (TRL 1) to a system proven through actual operational use (TRL 9). This framework can generally be applied to any technology and is a useful way to understand the maturity of the various gun safety technologies over the years. This framework was used in the 2005 NAE report and the same will be used here. Table 1 below reprints the TRL levels with their definition and descriptions from Section 2.5 of the April 2011 Department of Defense document.

Table 1. Technology Readiness Levels used to assess the maturity of technologies.

| TRL | Definition | Description |
|---|---|---|
| 1 | Basic principles observed and reported. | Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties. |
| 2 | Technology concept and/or application formulated. | Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies. |
| 3 | Analytical and experimental critical function and/or characteristic proof of concept. | Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative. |
| 4 | Component and/or breadboard validation in a laboratory environment. | Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory. |
| 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 they can be tested in a simulated environment. Examples include "high-fidelity" laboratory integration of components. |
| 6 | System/subsystem model or prototype demonstration in a relevant environment. | Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment. |
| 7 | System prototype demonstration in an operational environment. | Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space). |
| 8 | Actual system completed and qualified through test and demonstration. | Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications. |
| 9 | Actual system proven through successful mission operations. | Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions. |

## Technology Quick Reference Tables

While the technology assessment presented here is thorough and comprehensive, a proper assignment of TRL based on more in-depth analysis of each particular technology, prototype, or product was not the primary purpose of this report. To minimize any potential controversy associated with estimating technological maturity, the TRLs will be grouped into three tiers based on technological maturity and estimates will be made on this scale:

- Upper (TRL 7–9): Advanced Prototype or Production-Ready Design
- Middle (TRL 4–6): Breadboard or Experimental Prototype Design
- Lower (TRL 1–3): Basic Research or Component Design

The following tables below are provided for quick reference and contain many of the salient attributes associated with each technology development effort. They are grouped by tiers of estimated technological maturity. If sufficient evidence exists to make a more precise estimate of TRL based on the nine levels outlined in Table 1, it will be noted in the following section, Technology Developers. Any assignment of technological maturity, however, is only suggested based on the information and evidence that was available or made available for this report. Patents listed are not intended to be a complete inventory of intellectual property associated with each technology and are provided as a starting point for further research.

### Upper Tier

| Attribute | Description |
|---|---|
| Developer | iGun Technology Corporation |
| Technology Name | M-2000 |
| Product Type | Complete firearm |
| Firearm Type | Shotgun |
| Authorization Type | RFID |
| Development Timeframe | 1998–1999 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US006219952B1, US006282829B1, US006318134B1, US006343429B1 |

| Attribute | Description |
|---|---|
| Developer | Armatix GmbH |
| Technology Name | Smart System (iP1 and iW1) |
| Product Type | Complete firearm |
| Firearm Type | Pistol (.22 caliber original design) |
| Authorization Type | RFID |
| Development Timeframe | 2006–present |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US00D634806S, US007703229B2, US007908779B2, US20080244699A1, US20110061280A1, US20120151814A1, US20120180357A1, US20120329446A1 |

| Attribute | Description |
|---|---|
| Developer | Kodiak Industries |
| Technology Name | Intelligun |
| Product Type | Add-on |
| Firearm Type | Pistol (model 1911-style) |
| Authorization Type | Fingerprint |
| Development Timeframe | 2011–present |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US20130019510A1, US20130019512A1 |

### Middle Tier

| Attribute | Description |
|---|---|
| Developer | Colt's Manufacturing Company, Inc. |
| Technology Name | EP2 |
| Product Type | Complete firearm |
| Firearm Type | Pistol (modified CZ frame) |
| Authorization Type | Coded magnetic signal |
| Development Timeframe | 1997–2000 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US005704153A, US005867930A, US005896691A, US006237271B1, US006301815B1, US006363647B2, US00D387842S |

| Attribute | Description |
|---|---|
| Developer | Smith & Wesson |
| Technology Name | Authorized User Only Handgun |
| Product Type | Complete firearm |
| Firearm Type | Pistol |
| Authorization Type | PIN codes, grip, fingerprints, skin spectroscopy |
| Development Timeframe | 2000–2005 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US006286242B1, US006321478B1, US006345461B1, US006523296B1 |

| Attribute | Description |
|---|---|
| Developer | FN Manufacturing, Inc. |
| Technology Name | Secure Weapon System (SWS) |
| Product Type | Complete firearm |
| Firearm Type | Pistol (modified FNP-9) |
| Authorization Type | RFID |
| Development Timeframe | 2000–2006 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US006314671B1, US007356959B2 |

| Attribute | Description |
|---|---|
| Developer | New Jersey Institute of Technology |
| Technology Name | Child Safe Personalized Weapon |
| Product Type | Complete firearm |
| Firearm Type | Pistol (modified Beretta M9) |
| Authorization Type | Dynamic grip recognition, facial recognition |
| Development Timeframe | 1999–present |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US006563940B2, US006763126B2, US006817130B2, US007155034B1, US007278327B2, US008381426B2 |

| Attribute | Description |
|---|---|
| Developer | Metal Storm |
| Technology Name | O'Dwyer VLe |
| Product Type | Complete firearm |
| Firearm Type | Pistol (electronically fired, original design) |
| Authorization Type | RFID |
| Development Timeframe | 2002–2003 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US006477801B1, US007475636B2, US007743705B2, US007984675B2 |

| Attribute | Description |
|---|---|
| Developer | Safe Gun Technology |
| Technology Name | Not designated |
| Product Type | Add-on |
| Firearm Type | Shotgun (modified Remington 870) |
| Authorization Type | Fingerprint |
| Development Timeframe | Mid-2000s–present |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US006286240B1 |

| Attribute | Description |
|---|---|
| Developer | TriggerSmart |
| Technology Name | Not designated |
| Product Type | Add-on |
| Firearm Type | Pistol, rifle, shotgun |
| Authorization Type | RFID |
| Development Timeframe | 2010–present |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US008127482B2 |

### Lower Tier

| Attribute | Description |
|---|---|
| Developer | Sandia National Laboratories |
| Technology Name | Not designated |
| Product Type | Proof-of-concept demonstrators (pistol mounts) |
| Firearm Type | Pistol |
| Authorization Type | Voice, fingerprint, touch memory, remote RF |
| Development Timeframe | 1994–1996 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | None |

| Attribute | Description |
|---|---|
| Developer | University of Twente |
| Technology Name | Not designated |
| Product Type | Breadboard/prototype components |
| Firearm Type | Mock pistol |
| Authorization Type | Static grip recognition |
| Development Timeframe | 2003–2008 |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US20100272325A1 |

| Attribute | Description |
|---|---|
| Developer | Biomac Systems, Inc. |
| Technology Name | Not designated |
| Product Type | Add-on, license |
| Firearm Type | Unspecified |
| Authorization Type | Palm print, other biometrics |
| Development Timeframe | Near future |
| Relevant Patent Number(s) or Patent Application Publication Number(s) | US20110056108A1 |

## Technology Developers

The technologies are presented in roughly chronological order from when development began. The information contained in this section has been gleaned from several sources, including site visits, face-to-face meetings, telephone interviews, technology demonstrations, email correspondence, literature review, online investigations, and NIJ and BJA archival documents.

**Sandia National Laboratories.** In 1994, Sandia National Laboratories began to research and investigate the development of smart guns for law enforcement use.[35] The project was to specifically address the police takeaway problem where an adversary commandeers the service firearm of an officer and uses it to shoot the officer. Analysis of Federal Bureau of Investigation (FBI) data revealed that from 1979 and 1992 an average of 16% of the officers killed were killed with a service firearm, either the officer's own or another officer's, in the hands of an adversary, totaling 182 officers killed in 178 separate incidents during the fourteen-year period.

Sandia divided the research into three components. First, it sought to determine the requirements law enforcement officers would need in a smart gun. Second, it explored and evaluated different technologies that could help enable a smart gun. Third, it developed several demonstrator models that showed how various technologies could be used to secure pistols used by law enforcement. To determine the requirements, Sandia distributed a survey form to law enforcement agencies and received over 300 complete forms from respondents with different levels of law enforcement experience and differing responsibilities within their organizations.

In the 1996 report Sandia published, *reliability* was indicated as the most important concern by law enforcement practitioners.[36] The number of concerns that were categorized as related to reliability was almost three times that over any other category, and many of the other categories had hints of reliability in them as well. From this step, the user requirements were translated into a set of engineering requirements, or specifications. A

review of various technologies that could be used for authorization such as RFID and biometrics was combined with the specifications to create criteria for future R&D and to help design demonstrators to illustrate the various user authorization technologies. Some of these demonstrators are shown in Figure 1.


Figure 1. Various demonstrators produced by Sandia National Laboratories to illustrate the basic functionality of user authorization technologies, such as fingerprint (upper left), touch memory (upper right), remote RF (lower left), and voice recognition (lower right).

In 2001, Sandia published an update to the 1996 report where the researchers recapitulated the engineering requirements and discussed a number of non-technological issues such as legislative activity and manufacturing agreements at the time.[37] They also broadened the use of smart guns to include civilian uses and outlined a number of scenarios in both law enforcement and civilian contexts.[38]

**Colt's Manufacturing Company, Inc.** The Colt "Smart Gun" is a .40 caliber pistol which uses a coded magnetic signal technology to authorize or deny use of the gun based on the proximity of a transceiver device. Outwardly, the firearm does not appear any different than a regular handgun.[39] The authorization process begins with the user grasping the gun. The hand grip has a switch in it that, when depressed, initiates the authorization sequence. After the grip switch is depressed, the gun sends out a signal intended to be received by a transceiver device worn on the wrist of the user. Once the signal is received by the device, the device then sends a coded return signal to the gun. When it receives the coded return signal, the code is compared to a small list of "authorized" codes stored in the gun. If the code is authorized, a miniature motor is activated which in turn removes a blocking pin from the trigger mechanism, allowing the gun to be fired.[40] The basic operation is also illustrated in Figure 2. Colt had

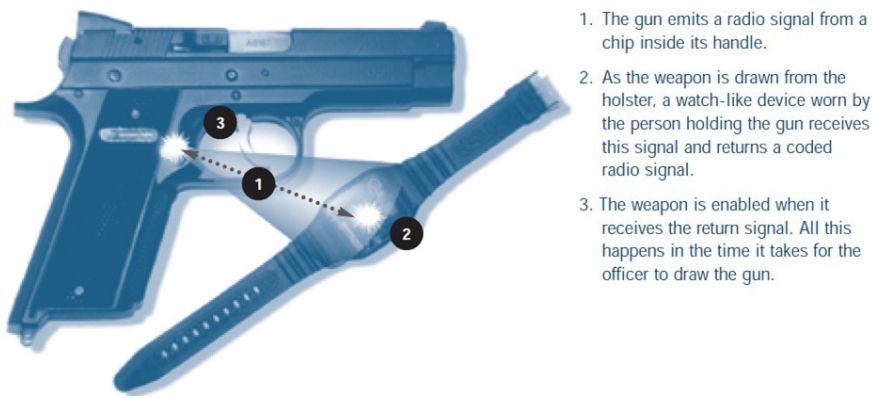


Figure 2. Basic operation of the Colt prototype (from reference 39).

considered using a design that would bypass the triggering mechanism so that excessive force on the trigger could not damage the blocking mechanism; however, a micro-motor trigger-blocking mechanism was found to be most energy efficient.[41]

In 1997, Colt began a three-year effort to develop a radio frequency Smart Gun.[42] The company had already spent $1,000,000 to develop an operational Smart Gun prototype dubbed the Evaluation Prototype 1 (EPI), which it used as a basis to develop an Evaluation Prototype 2 (EP2) with NIJ funding. Colt established goals for the EP2 design following both the results of an evaluation of various technologies published in the 1996 Sandia report and from an advisory board council of law enforcement personnel they convened. This redesign was envisioned to incorporate a much smaller transponder, an integrated power supply and radio frequency module in the grip, a laser aiming device, an improved blocking device, and a small on-board diagnostic display.

Figure 3. First of two Colt EP2 prototypes developed with SmartLinks and built on the .40 caliber CZ platform and delivered to NIJ.

Colt built two EP2 units based on a Česká Zbrojovka (CZ) platform, but also explored using a Vektor platform of South African origin. The CZ prototype units are shown in Figures 3 and 4. Colt partnered with a company called SmartLinks of Berkeley, CA, which developed the communications functionality for the EP2. While the EP1 used RF to communicate, the SmartLinks technology used a fluctuating magnetic field, which was more difficult to interfere with than an RF signal and was reported to be very low power to help prolong battery life. The system was controlled by a microprocessor programmed with custom software and integrated into the pistol and communicated via a wristband that enabled a mechanical actuator in the handgun when in close proximity. Up to four transponder codes could be used to accommodate multiple users, and that number could be increased through software modifications.

A solenoid was first tried as a trigger bypass for disabling the handgun; however, it was replaced by a miniature DC motor and lead screw assembly that drove a blocking bar into the trigger path to better achieve the design

Figure 4. Second of two Colt EP2 prototypes developed with SmartLinks and built on the .40 caliber CZ platform and delivered to NIJ.

goals. As the EP2 was only at the prototype stage, some of the load-bearing components in the blocking mechanism were not hardened. The guns were allowed to be test-fired anyway, and damage occurred to the non-hardened components. One of the prototypes was able to be repaired, but the other was damaged beyond repair. During testing it appeared that the SmartLinks locking system worked well, although the activation time was a little slower than initially desired (1/2 second as opposed to 1/4 second). Other issues surfaced during testing including issues with the grip switch and the software programming.

The prototypes demonstrated that it was possible to integrate the transmitter technology into a watch-size wristband and the wireless receiver and actuator into the handgun grip. The prototypes, however, were unreliable and not ruggedized enough to allow actual firing in an operational setting beyond the failed test fire, so reliability tests could not be conducted. It was envisioned that Colt would produce two prototypes to be delivered to NIJ and that NIJ would purchase an additional 20 units for field testing at two U.S. police academies.[43] In March 2000, Colt delivered its final report to NIJ on its development of the personalized firearm. Production of the additional units and field testing was not pursued, however. Colt subsequently made a corporate decision not to continue technology development and curtailed R&D in this area. Currently, Colt's Manufacturing Company LLC reports it is not pursuing further development of this technology at this time.

**iGun Technology Corporation.** The iGun M-2000 shotgun could be considered the first personalized firearm to go beyond a prototype to an actual commercializable or production-ready product. Developed in 1998, the iGun uses an ultra-low frequency RFID with inertia resistant blocking devices. Operation was designed to be transparent to the user. The operator wears a ring with an embedded passive RFID tag that responds with a specific code when energized by the RFID reader onboard the shotgun. If the code matches the firearm, a second verification is requested, and only if the second verification matches does the gun

enable the firing mechanism. Shown in Figure 5 below, the iGun M-2000 was designed as an integrated system and is not available as an add-on or a modification to a firearm already purchased or owned.[44] SSBT Center staff witnessed the M-2000 during a site visit in April 2013 and were allowed to fire the gun.

Figure 5. The iGun M-2000 shotgun (from reference 44).

iGun Technology Corporation was created as a subsidiary of Mossberg Group, Inc., a firearm manufacturer that specializes in rifles and shotguns. R&D was funded internally with a goal to create a personalized firearm as reliable as the most reliable shotgun. The concept behind the iGun began in 1995 and involved using magnets to prevent unintended gun use.[45] This led to prototypes that worked with magnets but were not "smart" as operation was affected by any typical magnet. The concept was revised in 1998 to use RFID technology.

The M-2000 was designed to operate in the exact way as a traditional firearm so that the user would not handle it differently. To fire the M-2000, the user depresses a lever built into the stock of the shotgun, positioned for the natural placement of a hand. The lever activates the electronics built into the stock of the gun, which broadcasts an RF signal at a maximum effective range of two inches. The gun looks for a response by the RFID chip embedded in a ring worn by the user. Two codes are requested by the gun from the RFID chip, and with over 18 billion combinations available

there is little chance for a misidentification. When the ring provides a response to the firearm, a user will hear a soft audible "click" (for both on and off) as well as a visual red indicator like those used in conventional firearm safeties as seen in Figure 5. However, this indicator will only appear after the unique code combination is matched between the firearm and the ring.

The M-2000 works as soon as handled (< 0.25 seconds), and the system turns off immediately when the user releases his grip of the firearm or when the RFID chip in the ring is removed from the two-inch proximity of the stock. This is intended to protect a user in the event that the shotgun is taken away and turned toward the authorized user. The M-2000 uses a patented dual solenoid design to block the trigger while the gun is not being used, which prevents bypassing due to movement of the gun, as opposed to more vulnerable single solenoid mechanisms. The M-2000 still utilizes a traditional manual safety and fails in a "safe" mode. The technology could be applied in such a way that law enforcement could have a single ring able to operate multiple firearms, multiple rings operate a single forearm, or even multiple rings operate multiple firearms. There is little chance the current M-2000 status indicators could be detected due to lack of installed illumination and the relatively short operating range. Both features could be important to law enforcement if the element of surprise was operationally relevant.

The battery was designed to operate through normal use for 10 years and is easily replaceable. Special custom-made batteries and circuitry warn of low voltage via an audible beep to give the user plenty of time to replace the battery. iGun reports that the firearm should be fully functional for a year or more after this initial notification to replace the batteries. In fact, iGun M-2000s built before 2000 with these batteries are still in operation to this day, according to the developer, including the one demonstrated to the SSBT Center. iGun considered the possibility of someone tampering with the firearm and noted that in nearly all cases of tampering, the firearm would be rendered inoperable. For example, removal of the electronic components or the locking mechanism would leave the firearm unable to

fire. Tampering with the system by using power to energize the firearm to try and force the system into an operational mode would likely burn out the electronics, as a person would need to have substantial knowledge of the system to power the locking mechanism. Additional security from gun tampering could be designed via special keys, pins, or screws.

In 2000, iGun contacted NIJ after developing the iGun M-2000 and received support to allow testing of the unit.[46] The unit passed MIL-SPEC 3433E, a 3,000-round buckshot torture test, and endurance and handling tests (NIJ Standard-0113.00 and ANSI/SAAMI Z299.5-1996).[47] iGun continued to run an internal battery of tests, and the result was only one failure of the firearm when mud jammed the standard mechanisms of the gun, preventing use. iGun applied 13,000 clicks of the "on" switch during testing in order to test the switch as well as the battery, and the system was still fully operational and unaffected. iGun indicates that their technology could be adapted to any number of other products or firearms. By starting with a firearm with such strong shock and impulse as a shotgun, migrating to other models should be easier. In addition, iGun did receive compliance for FCC rules Part 15 for the use of RFID.

Not unlike a traditional firearm, the M-2000 is not waterproof or completely impact resistant. If submerged, thoroughly soaked, or shocked from an unusual drop or impact, it should be examined and serviced if necessary. The susceptibility to corrosion of electronics is limited, as the electronics are enclosed away from commonly exposed places, although liquid immersions or salt spray (maritime environment) would have negative effects. The electronics are also housed away from areas that get cleaned and lubricated. If any gun were over-lubricated, however, it could affect proper functioning regardless of technology.

In order to gauge commercial interest, a marketing firm was hired several years ago to do customer research across the United States, including phone calls and consumer panels. The research found that while the concept of a personalized firearm was well received, few people would be interested in owning a personalized firearm. As of this writing, iGun noted

that the corporation has remained open, but the personalized firearm project has been shelved awaiting a change in market demand. The iGun estimates that enough components were created in 1998 to assemble 50 working units if ordered by a buyer. Currently, only a few of the key people who developed the iGun own personal copies and no other sales have been made.

In 2002, iGun undertook a project entitled *Personalized Firearm Research and Review of Biometric Technology* to research the potential of extending the design to include biometrics.[48] iGun partnered with West Virginia University to produce the report.[49] At the time, the research concluded that the implementation of a biometric was not feasible. However, the conclusion was made a decade ago and may not hold with more modern biometric technologies. In fact, Kodiak Industries and Safe Gun Technology, discussed in this report, have implemented fingerprint sensors into their designs.

**Smith & Wesson.** Smith & Wesson explored different methods of authentication including PIN codes, biometric fingerprints, and skin tissue spectroscopy approaches. Between 2000 and 2005, NIJ provided $3,673,361 to Smith & Wesson to develop a handgun that could only be used by an authorized user. Prior to the cooperative agreements with NIJ, Smith & Wesson reported to have internally funded a grip sensor that was incorporated in the handle of the handgun. By 2005, Smith & Wesson had also investigated electronic firing and reportedly tested over 60,000 rounds of electronically activated ammunition with prototype firearms with no limitations related to reliability or power sources.[50]

In 2000, Smith & Wesson began to advance its Smart Gun prototype which was designed to use biometrics and an electronic firing system to disable the firearm from use by an unauthorized user.[51] The project entitled *Development of an Authorized-User-Only Handgun* was split into two phases. Initial funding from NIJ supported an analysis of the existing electronic fire and combination lock system and a review and optimization of the existing design at the time for manufacturability and assembly.[52] Authentication was based on a PIN code authorization system initially.

Supplementary funding was used to examine the development and test of a nonintegrated fingerprint authorization system, creation of a prototype to explore "smart" component integration, and a continuation of biometrics technology research to meet law enforcement needs.[53]

Smith & Wesson extended its research and development to pursue development of a human skin biometric identification system called LightPrint designed by subcontractor Lumidigm, Inc.[54] The project entitled *Development of a Human Skin Biometric Identification System for Authorized User Only Handguns* was focused on maturing the technology Lumidign was developing in conjunction with Smith & Wesson. The additional funding by NIJ was provided to bring the LightPrint system to a point where it was to be incorporated into handgun access control applications. The ultimate goal of this proposal was to build and test a functional pistol prototype with an onboard LightPrint human skin biometric identification system. Although Smith & Wesson proposed the goal to deliver 50 prototypes for test and evaluation, reliably integrating the electronics into the firearm proved to be a challenge and ultimately only two demonstration items were delivered. A delivered prototype is shown in Figure 6.

Figure 6. Prototype developed by Smith & Wesson and delivered to NIJ.

**FN Manufacturing, Inc.** FN Manufacturing is a subsidiary of firearms manufacturer FN Herstal, headquartered in Belgium, and had already initiated a program to develop a smart gun in 1995 that focused on the law enforcement user.[55] Between 2000 and 2006, NIJ provided $2,606,156 to FN Manufacturing to develop an RFID-enabled handgun called the Secure Weapon System (SWS). FN structured its R&D for NIJ in four phases: (1) feasibility and functional requirements studies, (2) technical specifications, (3) operational specifications and recognition analysis, and (4) a working prototype. FN provided a comprehensive technical report on the SWS that included electronic designs, mechanical designs, the electro-mechanical interface, and system integration specifics. It also delivered production-like prototypes that represented the combination of selected specifications. The demonstration item used a ring worn on the finger that contained an RFID tag embedded in it and a receiver mechanism built into the handgun to prevent the firearm from firing when the ring was out of proximity.

In 2000, FN Manufacturing began to develop Phase 1 of its proposed four-phase R&D plan.[56] This stage was completed in June 2001. FN developed a demonstration unit which utilized ultrasonics to communicate between the firearm and an authentication device worn on the body. The initial breadboard concept utilized the FN "Five-seveN" 5.7 mm pistol and a wrist worn authorization device. Those were replaced by the "Forty-Nine Police Model" and a clip-on device worn like a pager on the body. The latter platform was chosen since it was deemed more relevant to police operations and came in .40 S&W and 9 mm versions. Ultrasonic sound was chosen because technology was better able to gauge proximity than other systems, was less sensitive to interference, and was highly directional in nature. Using a body-worn device allowed for more accurate authorization in the event that the user was wearing heavy clothing or gloves which may interfere with the ultrasonic signal if the device were worn on the wrist.

FN described the authorization process, which uses a combination of grip recognition and user authentication, in the following way:

> "*The grip switch unblocks the trigger and activates the electronics, the fire control is placed in 'secure' mode, and the recognition process with*

*coding begins soon after gripping the gun. When the recognition process between the gun and the PD* [personal device] *is complete and the user is authorized, fire control is allowed to be in the 'fire' position. The entire process, which occurs almost immediately, is complete and electronics are now consuming negligible energy from the battery. The user continues to be authenticated for as long as the grip switch is held, with no regard for the position of the gun in relation to the PD. This capability is a remarkable improvement from the earlier demonstration unit because once the user is authorized, the system no longer uses the ultrasonic communication to retain authorization. The user can orient the gun in any position without concern for losing authentication, so long as the user continues to grip the gun and thus the switch.*

"*Continuing to step through the process, the user releases the grip switch as the gun is returned to a holster. Since the gun was in 'fire' mode when the grip switch was released, the gun stays in 'fire' mode. No battery energy is used to return the gun to 'secure' mode. This is acceptable because, whenever the gun is gripped, the recognition process will again take place. For example, if an unauthorized person is next to grip the gun, that person will not be authorized, the fire control will disconnect, the gun will be in 'secure' mode, and electronics are consuming negligible energy from the battery. Conversely, when an authorized person is next to grip the gun, the fire control is placed in 'secure' mode, the person will be authorized again by the recognition system, and the fire control returns to 'fire' mode.*"[57]

This authorization protocol was used for the entire four-phase R&D cycle, although FN switched to an RFID-based system since there were potential downsides to using ultrasonics. It was noted that the highly directional nature of the ultrasonic technology would make placement of the body-worn device much more critical for communication with the firearm.

FN Manufacturing continued the SWS project with new support from NIJ.[58] Initial funding permitted the completion of Phases 2 and 3 in October 2002 and October 2003, respectively,[59] and supplementary funding supported

the completion of Phase 4.[60] FN developed the final design using the 9 mm FNP-9 as the platform, shown in Figure 7. Integrated into the handle was a fire control disconnection mechanism driven by a piezoelectric actuator, an RFID antenna, a grip sensor foil, and a printed circuit board for the sensor package, all powered by a lithium ion battery.

Several methods of packaging the RFID personal device were investigated in Phase 4, including rings, bracelets, special gloves, and others. In April 2004, FN Manufacturing entered a memorandum of understanding with VeriChip Corporation, a wholly owned subsidiary of Applied Digital Solutions, to examine the feasibility of developing an implantable RFID system for user authorized firearms.[61,62] Ultimately, a ring with an embedded passive RFID tag was chosen as the best candidate due to its size, concealability, versatility, and perceived level of acceptance. When worn on an authorized user's firing hand, the ring would be optimally located for reliable function and detectability by the SWS recognition and


Figure 7. The FN Secure Weapon System prototype built on the FNP-9 platform (from reference 63).

authorization system. An external master programming board is connected to the recognition system circuit in the gun to enroll new tags and perform other administrative tasks associated with the RFID functionality.[63]

As in the Phase 1 demonstrator, the technology of the final SWS prototype acts as more of a "de-authorization" system instead of an "authorization" system because the electronic locking system of the gun is normally in the "fire" mode as opposed to the "secure" mode once authorization has occurred. When a user grasps the firearm, he or she depresses a grip switch which initiates a signal to be sent from the firearm to a nearby RFID device. When the RFID device receives the signal, it in turn transmits a coded signal back to the gun. If the coded signal matches one of the authorized codes, it remains in "fire" mode. If the gun does not receive an authorized coded signal, then the electronics activate the piezoelectric actuator, which disengages a portion of the trigger link, placing the pistol in a "secure" mode.

Disengaging a portion of the trigger link allows the trigger to be fully actuated without the firearm being discharged. Since the trigger was designed to be free to move, excessive force on the trigger would not result in breaking or bypassing the locking mechanism. In addition, once the grip is released on a pistol that has been authorized, there is a one-second delay before subsequent grasping of the gun will initiate the authorization sequence again. This was done so it would be possible for a user to switch hands without having to reinitialize the authorization sequence.

FN Manufacturing produced four prototypes at the conclusion of Phase 4 in September 2006. Two were for delivery to NIJ, one was for delivery to FN Herstal, and one was retained at FN Manufacturing. One of the prototypes was tested by having 1,000 rounds shot from it using the following protocol:[64]

- The test is performed over 1,000 rounds, with a rate of fire not to exceed 1 round per second.
- All shooting will be performed with the gun and arms of the shooter unsupported.

- All malfunctions and part failures will be recorded and will be designated as Class I, Class II, or Class III as defined below:
  - Class I: A failure that may be immediately clearable by the operator within 10 seconds or less while following prescribed immediate action procedures.
  - Class II: A failure that may be operator clearable, requiring more than 10 seconds but not more than 10 minutes. Only the equipment and tools issued with the weapon may be used to clear the weapon.
  - Class III: A failure of a severe nature. The failure (1) is operator correctable but requires more than 10 minutes, (2) operator cannot correct and requires assistance (no time limit), or (3) requires higher level of maintenance, or authorized operator correction cannot be accomplished because of unavailability of necessary tools, equipment, or parts.
- Function of the piezoelectric actuator and SWS recognition system will be checked prior to the start of the test and at every 200-round interval.

After 600 rounds of testing, the first prototype began to allow an unauthorized test user to fire the gun due to a malfunction of the mechanical disconnection system. Testing was suspended, the prototype was examined, and it was discovered that one of the four screws in the grip hand worked loose and logged between the piezoelectric actuator and the aluminum frame. All screws were removed, cleaned, and coated with an adhesive before being placed back in the firearm. Testing was then resumed with no further incidence. Two additional prototypes to be delivered to NIJ were tested by firing 250 rounds from each pistol. No malfunctions occurred with either of these prototype units.

FN set the following system recognition goals: (1) a minimum 99.95% authentication for an authorized user and (2) a minimum 95% rejection of an unauthorized user. The protocol above included 100 authentication cycles. Combining the three test trials, the FNP-9 prototypes performed adequately with no authentication errors reported from 150 authentication cycles, meeting the imposed criteria. In addition, no firearm-related malfunctions or broken parts were reported in 1,500 rounds.

This effort would likely be categorized at a TRL 6 because the prototypes are beyond the breadboard stage and near the desired final configuration and the prototypes were tested in a relevant environment. In addition, the project appears to have been well-structured and well-documented. FN concluded in its final report to NIJ that while a number of technical advances had been made, further engineering and testing would be required to perfect the system. For example, the recognition time in the prototype took over 600 ms, which was demonstrated to lead to erratic behavior if the user attempted to execute actions too quickly and that blunt mechanical force applied to the side of the SWS firearm could override the electromechanically controlled blocking pin which would allow the gun to fire.

**New Jersey Institute of Technology.** A key feature of the NJIT system has been the use of dynamic grip recognition. Between 2004 and 2008, NIJ provided $2,515,475 in Congressionally directed funds to the New Jersey Institute of Technology to develop and demonstrate a technology for firearm user authentication based on DGR that built on initial work funded by the State of New Jersey.[65] From 2008 to the present, BJA has provided $1,504,818 in Congressionally directed funds to NJIT to further develop their technology. The proposed system was envisioned to incorporate information from both the hand shape and the dynamic pattern of pressure the hand applies to the handle during the first half-second of pulling the trigger to provide identification of an individual.

NJIT has focused on using existing popular models of pistols as a platform to develop its technology. It used a widely recognized Beretta pistol, commonly known as the M9 in a military context, as its platform based on recommendations from the U.S. Army Armament Research, Development and Engineering Center (ARDEC) and the Joint Service Small Arms Program (JSSAP) in Picatinny, NJ. NJIT attempted to develop partnerships with both Taurus and Metal Storm, two manufacturers of guns, but both the companies ultimately declined to participate.

The design of its Child Safe Personalized Weapon uses multiple pressure sensors located on the left and right grip pads of the gun located on the

handle. NJIT reports that the idea of using pressure came from research conducted on handwriting at AT&T Bell Laboratories. The pressure sensors are composed of piezoelectric materials that convert applied mechanical forces into an electric charge through a change in stresses in the materials where the voltage is proportional to the applied pressure. Each of these sensors built into the grip of the firearm measures the pressure applied by the hand at that position when holding the firearm. An array of these sensors is assembled to measure various pressures applied at different points on the grip, which in principle is different for each person and is interpreted as a unique biometric signature that can be used to authorize use of the firearm. This approach could potentially accommodate gun handles with complex nonplanar shapes using various pressure sensor arrays.

Building on preliminary efforts, NJIT worked to develop and demonstrate a technology for firearm user authentication based upon DGR with support from NIJ starting in 2004.[66,67,68,69] NJIT focused on developing a pressure transducer array that covered the entire gun grip and biometric pattern recognition algorithms to detect unique pressure signatures. A custom microprocessor supporting integrated digital signal processing and system control functions and microelectromechanical systems (MEMS) components for trigger motion detection were also developed. It was estimated that the electronics would require a 3.7 V and 600 mA battery to operate at this stage, and the power management goal was to achieve at least 24 hours of continuous operating time. NJIT miniaturized the hardware, software, and sensor systems to fit inside the handle of a Beretta and produced three prototypes capable of a single shot. At this stage, the prototypes did not incorporate an electronically controlled safety mechanism, so they only displayed a light that indicated authorization or no authorization rather than physically activating or deactivating the gun.

Starting in 2008, NJIT continued their research and development effort with support from BJA.[70] The technical effort focused on developing a disabling mechanism to integrate with the DGR hardware and embedded digital signal processing electronics. Gun disabling mechanisms were analyzed and evaluated for speed, power, size, marketability, and cost, which led to two laboratory evaluation prototypes for a mechanical and

electrical control system. Electrical ignition was considered potentially faster and more power efficient; however, the solenoid-based inhibition mechanism was considered more compatible with the existing gun market. A Beretta M9 handgun with integrated DGR hardware and firing inhibition mechanism was prototyped to operate on a standard 9 V alkaline battery power source that replaced more expensive custom lithium ion rechargeable batteries that could take several hours to charge. NJIT reported no problems after the solenoid-based prototype was tested with over 750 rounds of Simunition, a type of non-lethal training ammunition. The DGR algorithm was improved for accuracy, which NJIT reported reaching a positive recognition rate of approximately 97% for an authorized user and rejection rate of 98% for an unauthorized user using a small pool of subjects. Further independent research on DGR—both on the validity of the recognition method and with a more representative subject sample size—is likely needed before confirming DGR as a viable authentication method.

Work continued in 2009, primarily to relocate the safety components out of the magazine to free enough volume to hold at least nine rounds of ammunition.[71] At this stage, the magazine housed the electronics and solenoid, and the existing solenoid-based firing inhibitor was replaced with a new device located in the trigger linkage chamber. The new device used a spring made from a shape memory alloy called Nitinol and fit within the space constraints of the chamber. The associated driving circuitry utilized a photo relay as a switch to activate or deactivate the new device, and NJIT reported that a 300 ms pulse with a 9 V driving voltage was sufficient to activate the Nitinol firing inhibitor without causing any damages to the device and degrading the system performance. The new device was also reported to improve power consumption. Instantaneous power consumption of the solenoid was close to 5 W, or equivalently drawing 0.55 A, which quickly exhausted the alkaline disposable battery in about 10 rounds of firing. The Nitinol system was reported to handle more than 100 rounds of firing with a standby time of 24 hours. New electronics to fit into both sides of the handles as well and a greater density of sensors were explored to address the potential variations in grip in a large population of users.

From 2010 to the present, NJIT has continued to further develop the Nitinol spring firing inhibitor and electronics and has explored the addition of a face imaging and recognition system.[72] A prototype with a five-round capacity built on the Beretta platform with integrated conformal electronics built into the grips contained 28 pressure sensors to increase the sensor density to provide more detailed biometric information, as shown in Figure 8. A face recognition system was also explored as a part of the firearm system, but the computation associated with facial recognition was accomplished on a desktop computer rather than onboard the gun. NJIT expects that the increased sensor density along with DGR and the face recognition functionality or other independent, complementary biometric sensor system will significantly enhance the user identification. Currently, this project remains ongoing.

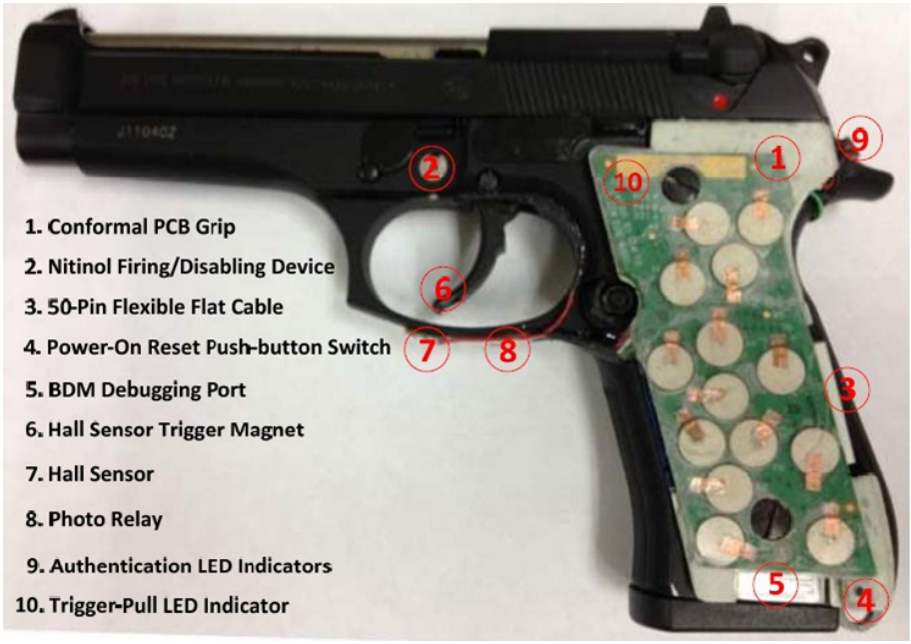


Figure 8. NJIT prototype currently under development (from 2010-DD-BX-K541 award file).

NJIT has teamed with ARDEC to update the technology prototype. Proposed work includes an upgrade of the CPU from a 10-year-old automotive processor chip to reduce power consumption and increase computational speed, use of conformal batteries to make available space taken from the magazine by the 9 V battery currently used, and general redesign for manufacturability and durability in the field. The system will be designed onto a Sig Sauer P228 or P226. ARDEC plans to conduct the testing utilizing its existing facilities. An operational goal is to have a "failure to feed, fire, or recognize" be 1 in 1,000. Development of five units is expected for demonstration and testing purposes with the desire to obtain follow-on funding for 50 to 100 units.

**Metal Storm.** Metal Storm Limited is an Australian company based in both Brisbane and Arlington, VA, that specializes in electronically-fired weapons for military and law enforcement applications. In 2002, it investigated the further development of a handgun already under development that was fired entirely electronically.[73] The concept pistol, called the O'Dwyer VLe (which was a shortened version of *V*ariable *L*ethality), came in two designs.[74] One had a single barrel and one had multiple barrels that could accommodate less lethal rounds such as small beanbags as well as serially stacked ammunition that was fired electronically.

The VLe did not have a conventional magazine. The bullets were designed to be stacked in-line in the barrel and ready to fire. The working prototype was a seven-shot single barrel unit that could fire multiple rounds with a single pull of the trigger. Metal Storm provided a video that demonstrated the functionality of the prototype designs. Figure 9 shows the single barrel unit and a computer rendering of the multibarrel design. The pistol grip contained three electronic subsystems. One subsystem operated the firing mechanism, another provided audio and visual confirmation of settings, and the third provided authorization to use the gun. Figure 10 shows a computer visualization of the lethal and nonlethal rounds discharging from the multibarrel design.

Metal Storm incorporated many requirements for smart guns from both the 1996 and 2001 Sandia reports in the design of the VLe and only had a law enforcement user in mind for the product. The gun utilized an RFID authorization system with a chip embedded in a ring that the user wears on the firing hand. It noted that the keying system could activate the gun in just tens of milliseconds when the code sent by the transponder matches


Figure 9. Stills from a video submitted by Metal Storm to NIJ that demonstrate the functionality of the prototype designs. The Metal Storm VLe concept pistol showing the single barrel unit (upper left) and a computer rendering of the multibarrel design (upper right, lower left) that could have both lethal and nonlethal ammunition loaded in different barrels. A switch (lower right) would allow the user to switch between lethal and nonlethal options.

one in the gun's memory. The original design also required the use of ammunition specific to Metal Storm systems. Metal Storm stated that the specialty ammunition would only be available to a limited customer base, which it suggested would reduce the value of the gun to unauthorized personnel, reduce the motivation for theft, or both.

Metal Storm stated it had no plans to make a consumer version of the VLe but instead would focus on law enforcement and military systems development and implementation. In its final report to NIJ, Metal Storm outlined its recommendations for the engineering steps that would be required to take the concept to a tested, working product. Given appropriate support, it estimated that the VLe system could be ready for field trials in as little as 18 months, with the first systems in the hands of law enforcement within two years. Further funding was not forthcoming, and Metal Storm has since not pursued any additional development of the VLe.

Figure 10. Computer visualization showing the ammunition stacked in line. A lethal round can be fired (left) or a nonlethal round can be selected (right). Stills from a video submitted by Metal Storm to NIJ that demonstrate the functionality of the prototype designs.

**University of Twente.** The University of Twente in the Netherlands has researched a static grip recognition methodology for handgun authorization.[75,76,77,78,79,80,81,82] Using a 44 × 44 piezoresistive pressure sensor on the hand grip of a mock handgun and data obtained in cooperation with local authorities, it has developed algorithms designed to have a 1 in 10,000 failure rate with a 1 in 10 probability that an unauthorized user would be able to fire the gun ("false accept rate" of 10%). Static "images" were recorded from trained police officers and untrained individuals by having the subject grip the gun and verbally indicate when he or she was in the proper firing position. "Images" were collected based on the placement and the amount of pressure on the 44 × 44 element sensor. These images were then used to help verify and develop algorithms intended to keep an unauthorized user from firing the gun. The desired performance target was not obtained, but the researchers make recommendations for further improvements, including the design of a customized pressure sensor and improvements in the data analysis. This technology is still in the research phase with a focus on the algorithms for authorization. In addition, the technology has not been integrated into a firearm and is still at the component testing level without integration of the different components into a complete system.

**Armatix GmbH.** Armatix has developed the Smart System, a user-authorized firearm system that consists of an originally designed handgun (iP1) and a wrist-worn transponder (iW1) that is used to authorize the firearm and user.[83] The Smart System uses active RFID to establish communication between the wrist-worn transponder and the firearm through communication in the Rayleigh region, which is more resistant to interference. Furthermore, the transponder requires a personal identification number code to be input before it will transmit an authorization signal to the firearm, similar to a code used with an ATM card. The Smart System is currently a commercial system with Armatix reporting units sold in Europe and Asia. Armatix has also taken necessary steps to allow for the importation and sale of the Smart System in the USA.

The iP1 is a .22 caliber double action pistol with a 10-round magazine, as shown in Figure 11. Armatix designed the gun in order to fully integrate the user authorization system at the design level, instead of attempting to incorporate the authorization system into an already commercially available firearm. The pistol uses an integrated blocking mechanism which will allow it to fire only if the gun receives an authorization signal from the wrist worn transponder. Synchronization between various mechanically and electronically controlled components in the iP1 is required to allow it to fire. Armatix reports that in order to defeat the blocking mechanism, re-engineering and construction of the pistol slide would be required in order to circumvent the necessary synchronization.


Figure 11. Armatix iP1 .22 caliber pistol (image from online FCC report in reference 87).

The wrist-worn component of the Smart System authorizes the user via a five-digit PIN code, and it also looks like and functions as a digital watch (see Figure 12).[84,85] To activate the system, the user inputs the PIN code by using four buttons on the face of the watch. If the PIN code is incorrect, "FAIL" will appear on the watch display. If the PIN code is correct, "GOOD" will appear on the watch display and a "remaining time" for authorization must be entered (eight hours maximum, one hour minimum).[86] The watch then sends a signal to the pistol allowing it to be fired for the specified amount of time. Once the set time has expired, the pistol will deactivate. The pistol can also be manually deactivated before time has elapsed. The pistol will also deactivate if it is moved beyond the range of the watch (15 inches) and will automatically activate again when brought back to the activation distance. Note that when batteries are first inserted into the


Figure 12. Armatix iW1 wrist unit (images from online FCC report in reference 88).

Smart System (two standard AAA in the pistol and CR2032 in the watch), the watch and the pistol must be synchronized, a procedure that takes a few seconds. An LED display on the firearm indicates the following status:

- Blue – No magazine inserted (gun will not fire even if a bullet is in the chamber)
- Red – Gun not ready for firing (unauthorized or not synchronized)
- Green – Gun ready for firing
- Blinking indicator – Low battery

The watch and the gun must have matching PIN codes, which are provided to the customer on PIN safety cards. If a watch is lost or destroyed, a new watch must be reprogrammed with the PIN code of the gun. For police applications, it is possible to have one watch authorize more than one firearm as well as having one firearm operated by more than one watch.

Armatix GmbH is a German company and a spinoff of SimonsVoss AG, which specializes in wireless mechatronic locking and security systems. It also produces other products including the Quicklock, a "down-the-barrel" locking/blocking device that inserts into a gun barrel through the muzzle, and the Baselock, a secured holder for guns. Armatix outsources the manufacturing of the individual components and then assembles the finished product in their factory in Petersberg, Germany. In April 2013, the SSBT Center visited both the corporate offices in Munich and the production facility in Petersberg. SSBT Center personnel observed the operation of the Smart System and were allowed to test fire the gun. It functioned as intended, firing when an authorized user attempted to fire it, and not firing for an unauthorized user. A total of 10 rounds were fired through the pistol without any malfunctions or misfires.

Armatix is pursuing approval for commercial sale in the United States through their U.S. subsidiary Armatix USA and expects the Smart System to be offered for sale by midsummer of 2013. Armatix has submitted the Smart System for testing in laboratories for certification by relevant authorities and organizations such as the Bureau of Alcohol, Tobacco,

Firearms and Explosives (ATF), the Federal Communications Commission (FCC), and state agencies in California and Maryland. The FCC governs the transmissions of electronic devices and requires certification of all intentional radiators for use in the United States. Since the pistol and the wrist watch are both considered intentional radiators, these required testing in an FCC-approved laboratory for regulatory compliance with FCC Rules 47 CFR Part 15. The pistol (FCCID ZYXSMARTIP1)[87] as well as the watch (FCCID ZYXSMARTIW1)[88] were tested at the FCC-approved testing laboratory EMCE GmbH in Burgrieden, Germany, and were found to be compliant to the applicable FCC regulations.

The Armatix iP1 semiautomatic pistol has qualified for importation into the United States by ATF. It had been submitted to ATF for examination and classification regarding importability into the USA, but initially the firearm was determined to be non-importable because it was not able to accrue the minimum 75 points necessary on ATF Form 4590 "Factoring Criteria for Weapons." Based upon these findings, Armatix incorporated design changes to the iP1 pistol in order to produce a firearm suitable to import into the USA. Main changes were made to the internal fire control components by welding them into a single receiver and enlarging the window used as a loaded chamber indicator.

After making the design changes, Armatix resubmitted the pistol for examination and classification by ATF. On December 22, 2011, ATF reported that the design changes Armatix made allowed the gun to accrue 80 points on ATF Form 4590 and stated that the pistol is recognized as particularly suitable for, or readily adaptable to, sporting purposes and may be imported into the United States for commercial sale.[89] However, it was emphasized that additional markings would be required on guns imported into the United States intended for sale: specifically, the country of origin and the importer's information must appear on the gun. These may be applied by either the manufacturer or the importer.

Armatix has also completed testing required for all handguns manufactured in or imported into California with the intention to be sold. United States

Test Laboratory (USTL) in Wichita, Kansas, a division of National Technical Systems, conducted testing required by California Penal Code Sections 31900 through 32100, and on January 24, 2013 USTL reported that the three sample Armatix iP1 pistols met the required specifications.[90] Tests included conformation of a positive manually operated safety device [Penal Code section 31910, subdivision (b)(1)], firing tests, and drop safety tests.

Firing tests require the first 20 rounds be fired without a malfunction that is not due to a faulty magazine or ammunition as well as firing 600 rounds with no more than six malfunctions that are not due to a faulty magazine or ammunition. It is also required that after 600 rounds there be no crack or breakage that would increase the risk of injury to the user. Drop tests require that the weapon be dropped from a height of 1 m + 1 cm without firing in 6 specific orientations:[91]

1. Normal firing position (barrel horizontal)
2. Upside down (barrel horizontal)
3. On grip (barrel vertical)
4. On muzzle (barrel vertical)
5. On either side (barrel horizontal)
6. If there is an exposed hammer or striker, on the rearmost point of that device, otherwise on the rearmost point of the handgun

On January 24, 2013, USTL also reported that it had submitted a Compliance Test Report on the iP1 as required by the California Code of Regulations, Title 11, Section 4052. Armatix reports that the regulatory process is ongoing and further steps beyond testing are required before a company is listed on the California "Roster of Handguns Certified for Sale," which would permit a firearm to be offered for sale in that state.[92] Armatix already has three varieties of its Quicklock devices listed on the California "Roster of Firearm Safety Devices Certified for Sale."[93]

Armatix has also submitted the gun for review by the Handgun Roster Board in the state of Maryland, which must approve any firearm offered for

sale manufactured after 1985. NIJ and SSBT Center staff observed a test firing of the Smart System at the Maryland State Police Forensic Science Laboratory in February 2013, which occurred as a part of the Maryland regulatory process. Multiple pistol units were present for visual inspection as shown in Figure 13. Per the testing protocol, one example firearm discharged the first 20 rounds without malfunction, although some user difficulties were observed with the initial synchronization between the gun and the wrist-worn device which were resolved. Figure 14 shows the red and green lights demonstrating unauthorized and authorized states of the Smart System, respectively.

Armatix reports ongoing development projects for bolt-action rifles, semi- and fully automatic rifles, breakdown rifles, shotguns, and revolvers. Armatix reports that it has tested a 9 mm pistol and a .44 caliber revolver

Figure 13. The Armatix Smart System showing the iP1 pistol, magazine, and the iW1 communicator worn on the wrist as presented at a test firing of the Smart System at the Maryland State Police Forensic Science Laboratory in February 2013.

and anticipates making these models commercially available in the future. The SSBT Center observed engineering drawings of a 9 mm pistol during a site visit in April 2013. An earlier version of the iP1 and a concept revolver with Smart System technology were previously reported to be on display at the 2010 Shooting, Hunting, Outdoor Trade Show (SHOT Show) held in Las Vegas, NV.[94] The annual SHOT Show is owned and sponsored by the National Shooting Sports Foundation (NSSF) and billed as the largest and most comprehensive trade show for all professionals involved with the shooting sports, hunting, and law enforcement industries.[95] As a result of the Smart System development process, Armatix also reports that the technology used in the iP1 could be provided to gun manufacturers as an "original equipment manufacturer" (OEM) solution. It reports working with gun manufacturers to incorporate its technology and licensing negotiations with interested parties.

Figure 14. Indicator lights on the iP1 showing the firearm in an unauthorized state (red) and an authorized state (green) during a test firing of the Smart System at the Maryland State Police Forensic Science Laboratory in February 2013. Permission to use images granted by Maryland State Police Forensic Science Laboratory.

**Safe Gun Technology.** Safe Gun Technology (SGT), based in Columbus, GA, has developed a prototype user-authorized version of a Remington 870 shotgun with an authorization system that utilizes a fingerprint identification sensor module. SGT prevents the operation of the shotgun by disabling the firing pin using a split firing pin design that allows the hammer to drop normally but on the disabled side when not authorized. The SGT system utilizes an "authorize once" approach to arm the gun, which remains in an armed status as long as a hand applies pressure to the grip. If pressure is released on the grip or the gun is dropped for longer than one second, the system de-authorizes. No finger is necessary on the scanner after initial authorization, provided pressure to the grip is maintained. The prototype is shown in Figure 15.[96]

The SGT system is being designed to allow for recharging in a cradle. When the batteries are running low, a red indicator light will flash. While in this state, enough power remains to authorize and relock the gun approximately 20 to 30 times. If the battery fails or becomes too low to operate, the SGT prototype will fail in a "secure" state and has non-volatile memory that keeps the fingerprint database intact. The system also has a "hot point" power connection where a user can connect an external 9 V battery to provide temporary power to release the lock through a fingerprint or PIN code typed on a keypad. If the power fails while the gun is enabled, it will

Remington Model 870™ Shotgun (with modified pistol grip) shown with SafeGun™ User-Authorized Kit prototype installed.

Figure 15. Modified Remington Model 870 shotgun by Safe Gun Technology (from reference 96).

remain disabled until power returns. This system is constantly "on" while out of its cradle, which has prompted SGT to design a secondary battery into the system as a backup and perform an audit of the power system. SGT investigated but discarded plans for user-replaceable batteries in order to ruggedize the unit with packaging and waterproofing.

SGT designed the system to only be modified by an expert that has been trained on the specifics of the technology. A user with administrative control can add additional users with a combination of a master fingerprint and a sequence of keystrokes on a keypad, although SGT indicates that future versions of the technology will allow configuration on a computer via a USB connection. SGT reports it is actively working on options to replace or augment the fingerprint sensor with additional sensors, such as iris, palm print, and thermal, and to miniaturize system components to migrate to any size or style of firearm. It intends to develop a means of altering the mechanical lock, chamber loading, firing, ejection, reloading, and cycling that would make tampering for conventional use prohibitively expensive and extremely time consuming even for professional gunsmiths.

SGT has internally performed functionality and electronic interference testing as well as live-round testing, including multiple master-authorized and user-authorized firings. SGT reports that its goal is to add subsystems with reliability factors that do not diminish the overall reliability of the firearm. SGT has stated that it is working toward a system with a "false reject rate" (FFR) of 1% and a "false accept rate" (FAR) of 0.0001%. The FRR and FAR values are provided by a biometrics partner that has implemented the same system in other products.

Future testing is reported to include all necessary safety and handling tests, such as drop tests, misfiring, and jamming. Although SGT reports that it is not aware of any current standards with respect to user-authorized firearms or add-on devices, it is aware of various tests such as the ANSI and SAAMI drop and cocked hammer tests in five directions. SGT stated it is modeling its testing, failure risk analysis, and quality system methodology after U.S. Food and Drug Administration (FDA) medical device protocols, given past

experience in that field. The company design team is comprised of veterans of the medical field with expertise in miniaturization and reliability design and testing. SGT has not yet performed rate of failure statistics on the mechanical system.

SGT reports that it is presently pursuing several research activities related to the mechanical and authorization subsystems, including multiple component locking methods. SGT is in the process of redesigning its system into an integrated system with a specially manufactured stock mold. SGT's system has five sockets that will be sealed with oil-resistant seals and three electronic boards that will be encapsulated in molded polymeric casings for additional protection. Since the prototype is a standalone device, SGT is considering incorporating a programmable logic controller (PLC). This functionality would allow manipulation of various settings in the firearm through a computer connection, thus enabling an armorer or officer to authorize and de-authorize firearms under his or her supervision. Furthermore, it envisions that this could allow its technology to be pre-programmed to function according to the tailored usage requirements of law enforcement, civilian users, or military operators.

All modified shotguns are prototypes and are only in use by SGT's R&D team. Although current design plans are focused on law enforcement, this technology could be used by the general public. To date SGT has not partnered with any outside entity, but reported that it is willing to consider various forms of collaboration. The SSBT Center was unable to observe the prototype or a physical demonstration of the prototype during a site visit due to the unit being in a different location.

**TriggerSmart.** TriggerSmart is an Irish company, based in Limerick, that has produced prototypes of RFID-based user authorized firearms.[97] TriggerSmart partnered with Georgia Tech Ireland—a satellite research institute affiliated with the Georgia Institute of Technology—to bring the technology to the prototype stage. The electronics in the firearm are housed in the gun handle, and an RFID chip can be worn in a ring or bracelet or could even be implanted in the hand of an authorized user.

TriggerSmart has looked at other technologies, but found that RFID would be the best fit for its applications. The token can take several forms, but currently a ring is preferred.

The firearm portion of the TriggerSmart system will be a user replacement part. For example, to convert a rifle to the TriggerSmart system, the user would replace the factory-installed lower receiver with a lower receiver designed by TriggerSmart. It has built three demonstration firearms—a handgun, a rifle, and a shotgun—and reports that it has successfully fired the guns over 1,000 times. SSBT Center staff observed the semi-automatic MP5 with a TriggerSmart lower receiver shown in Figure 16 during a site visit in April 2013. The technology has not been tested beyond the prototype stage, nor has it been tested by a third party. The technology, however, has been integrated into reasonably realistic, fully-functional demonstration models. The company indicated that the handgun is no longer available for legal reasons.

The patented system uses passive, low-power 13.56 MHz high frequency (HF) RFID in order to eliminate the battery on the tag and operate in an "instant-on" state. The system uses near field communication technology,

Figure 16. A semi-automatic MP5 with TriggerSmart lower receiver as presented at a site visit in April 2013.

which reduces the amount of interference the system could experience. The system's electronics, antenna, and batteries are located within a handgrip, which emits a low power signal in the Industrial, Scientific, and Medical (ISM) bands that powers the RFID tag on the token. The system uses an ultra-low-power microcontroller to provide control of a miniature motor seen above the handle on the side of the firearm in Figure 16. The microcontroller periodically checks with a HF RFID radio receiver to see if any tags are present. If an authorized RFID tag is detected within range, the microcontroller then sends a signal to the motor which removes a blocking device from the trigger bar, thus allowing the gun to be fired. A motor allows the system to lock the firing pin of the firearm and render it inoperable. When RFID contact is lost, the blocking device is activated within half a second; however, this response time can be tuned by TriggerSmart to be shorter or longer depending on the user application. The default operation of the motor is a failsafe position where the firearm is locked, but could be modified to fail open where the firearm is active by default.

The inductively coupled HF RFID system uses a 6.2-cm diagonal rectangular, four-turn wire loop antenna.[98] The antenna is mounted to the rear end of the firearm's grip. Based on previous research,[99,100] the antenna was spaced as far as possible from the metal surface and made as large as possible to allow the most magnetic flux to loop around the firearm grip in order to optimize the communication between the RFID reader and passive tag. TriggerSmart is also investigating approaches to increase the communication distances of their products.[101] To minimize the power consumption of the microprocessor and RFID reader, TriggerSmart notes that querying tags as infrequently as possible is an important system design factor. TriggerSmart based its query time on research on average human reaction time to visual and auditory stimuli, which is noted as 190 ms to react to light stimuli and 160 ms to react to sound stimuli.[102] It proposes that the reader system should search for a new tag on the order of 160 ms in order to maximize sleep time and thus battery life onboard the gun.

**Kodiak Industries.** Kodiak Industries is a national and international distributor of shooting sports and outdoor products based in Salt Lake City, Utah, that carries feature brands as well as internally developed firearms.

Kodiak Industries launched a biometrically enabled firearm called the Intelligun in 2012 and considers it an accessory that provides an additional layer of security above that of a standard firearm. Intelligun is a fingerprint-based locking system installed on a model 1911-style .45 caliber handgun that uses a patented design to completely lock the gun from operation when not in use while unlocking it immediately (in a fraction of a second) for authorized users. SSBT Center staff witnessed the Intelligun system on a .45 caliber unit during a site visit in March 2013.

Intelligun is composed of a shielded, enclosed grip and main spring that replaces the standard grip and main spring, combined with special safety screws to prevent system tampering. The unit is sealed, chemically resistant, and water resistant with future plans for waterproofing. The Intelligun system utilizes a Department of Defense–approved, Cisco-certified fingerprint sensor. Once Intelligun is installed, the system cannot be readily converted back to operational usability without substantial firearm knowledge and parts. Persons trying to tamper with the system to energize the electronics to an operational state will cause a system failure as the circuitry is sensitive to the supplied power. Kodiak reports that the unit does not broadcast or create any form of an electronic signature that could be detected. The total weight of the add-on component will add an equivalent weight of less than one round to the total weight of the firearm. A pistol with the Intelligun system installed is shown in Figure 17.[103]

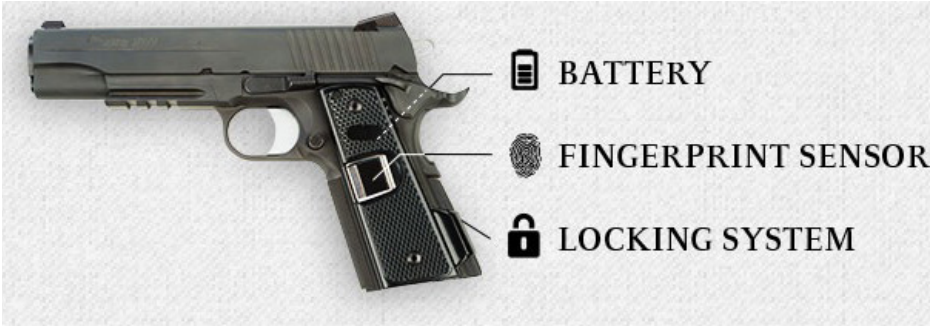


Figure 17. Intelligun system featured on a model 1911-style pistol (from reference 103).

The system turns on when a person applies pressure via the gripping of the handle via pressure sensors installed in the grip, a natural process when removed from a holster or gripped in a hand. A user of the system would likely have enrolled the middle finger as this is the natural finger for placement on the biometric sensor as shown in Figure 18. As soon as the system has completed booting, it reads the fingerprint and compares it to authorized users. The system will remain operational as long as it remains in the grip of the user. The whole process takes a fraction of a second and does not occur multiple times during use. It only occurs during the initial gripping after being picked up or removed from a holster. In the time it takes a person to draw and aim the firearm, the system has booted and identified whether a user is authorized to fire the system.

Intelligun also has a pressure-based safety grip that functions as an operational safety for the system by disabling the ability to fire the gun as soon as a person's grip is released. The duration that the system remains

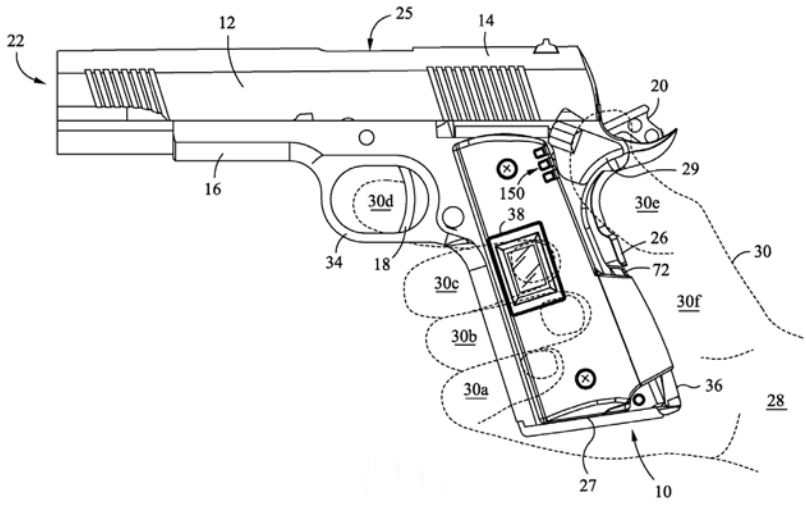


Figure 18. Natural hand placement illustrated on the Intelligun system from United States Patent Application US 2013/0019510 A1.

operational from when an authorized user stops gripping can be adjusted. The firearms will enter into a "high security" mode if a non-registered person tries to use it multiple times (3x). In order to return the firearm to an operational state, the administrator must re-enable the system through a specific sequence of steps. The unit has three light-emitting diode (LED) status indicators—red, yellow, and green—to provide system status, battery life, and operational information. A button provides a system and battery status display. When this button is pressed and held, it will dim the LED indicators for night use, and the process is repeated to return to daytime operation.

After purchase, the first person to grip and place a finger on the fingerprint sensor begins administrator enrollment in the Intelligun system. The company notes that there is only one administrator, and only the administrator can add new users. During the administrator initialization and any new user additions, the Intelligun system will require multiple (three to five) fingerprint captures to properly enroll a person. This will allow the system to better recognize a fingerprint even if it is not fully or directly on the biometric sensor at the time of use. However, it is always recommended to try and have a fingerprint fully on the sensor. If desired, the firearm administrator can perform a system wipe that will remove all users except said administrator. Only a factory reset of the system can completely remove all users including the original administrator returning the system to an unregistered state, with no active users.

Kodiak Industries reports the lithium ion battery should last about a year between charges, based on two to three uses a week (or approximately 800 hours). It charges via a standard micro USB port. The system's failsafe mode is a closed or non-functional state. Intelligun has a manual override installed that operates via a special key that with a quarter turn allows use of the unit. This is not unlike locks that are built into many firearms available today, although it should be noted this would override the failsafe mode and allow operation when the battery is dead.

Kodiak Industries chose to develop the Intelligun system for a model 1911-style handgun for its initial outing. The system was designed to work on any 1911-style handgun regardless of the caliber due to the standard frame and assembly. A detailed view of the components is shown in Figure 19. Kodiak stated the first release of the Intelligun will be a factory install only. In the future, dealers may be able to take an installation class and be allowed to install and warranty the product. Additionally, if a purchaser sends the firearm to Kodiak Industries for an install over a dealer, they will receive an additional year of warranty. Its plans for developing an installation of Intelligun for other handgun models will be addressed as the market demands. The system requires a left- or right-handed installation due to sensor and indicator positioning, although Kodiak indicated plans to

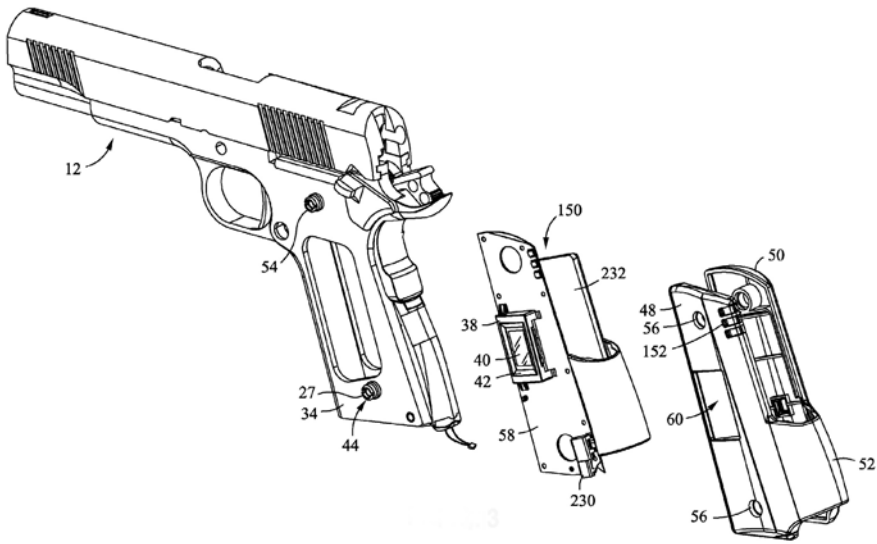


Figure 19. An exploded view of the Intelligun hardware to modify a 1911-style pistol from United States Patent Application US 2013/0019510 A1.

develop an ambidextrous version of the system as technology progression allows and has looked at what would be required to place the system on rifles, revolvers, and other firearms. User logging or GPS features could be designed into the system if the market demand called for the functionality, but they are not part of the current Intelligun unit.

Original development of the system was aimed at law enforcement and military, and Kodiak Industries indicates that it has explored the use of Intelligun for airline security and corrections applications. Intelligun's marketing includes families looking for safer firearm options. Kodiak stated that it can manufacture 50,000 units per month and has plans for a call and service center for the Intelligun. SSBT Center staff toured the manufacturing and planned service center areas in Utah in March 2013. Kodiak Industries reported plans to begin beta testing of Intelligun in April 2013. It reports that it is currently taking advance orders with the expectation of a shipment later in 2013. It also noted that it debuted the Intelligun at the 2013 SHOT Show in Las Vegas, Nevada.

Kodiak plans to have standard handgun operational testing completed for normal firearm use. It is also working on testing parameters for applications where the electronics subcomponents in the unit are required to meet U.S. military standards (i.e., MIL-SPEC) and developing its own testing parameters in the absence of a standard for user-authorized guns promulgated by an official entity like a standards development organization. Plans include system testing for withstanding extreme temperatures as well as within a narrower temperature range where most operational use would be expected. Kodiak explored various existing standards to create the test plan. It reports that the Intelligun system is expected to have a less than 1 in 10,000 failure rate. Kodiak reports that it is expected that standard class 1, 2, and 3 firearm failures will happen more often with the pistol that the Intelligun system is installed on than electronic failures associated with the safety technology.

**Biomac Systems, Inc.** Biomac Systems, Inc., was incorporated in Delaware to develop biometric access control for handguns through producing retrofit kits, licensing Biomac technology to firearms manufacturers, supplying sensor modules and parts to firearm manufacturers, and establishing retrofitting centers to convert existing firearms into smart guns that limit the use of the guns to authorized persons.[104] Biomac reports forming strategic alliances with Austrian and German experts in the fields of gun making and biometrics and reports plans to develop a retrofit kit for firearms to add user-authentication to existing firearms, although no physical device or modified firearm has been produced yet. Although the planned system is envisioned to use palm print biometrics for recognition access, Biomac indicates plans to design a sensor system not to operate solely on palm prints as the patented technology permits multiple sensors in the sensor array.

Biomac reports a goal to use multiple parameters to work toward a 99.99% accurate system and for the system to recognize an authorized user in less than one-quarter second. It will have provision for up to 11 authorized users. The electronic components are envisioned to have extremely low demands for electrical current so that the system's built-in battery will be sufficient for two to three years of system readiness. Biomac has formed a contractual alliance with HTBL-Ferlach in Austria that is anticipated to result in the complete engineering of the pistol retrofit kit for use with the electronics control module yet to be developed.[105] Biomac notes that it ultimately anticipates placing handgun retrofit kits on the market at a price point between low-tech gun accessories and high-tech gun safety products like fingerprint-activated gun vaults.

The technology that forms the foundation for Biomac's proposed sensor system is image sensors that are developed and manufactured on organic or polymer materials that can be directly printed on low-cost, flexible substrates. The manufacturing technique is similar to inkjet printing, commonly used for printing documents onto paper, but instead uses a

metal or semiconductor colloidal ink to deposit optoelectronic materials on various flexible or odd surface materials. The central component of Biomac's planned user-authorized firearm system is a multimodal biometric sensor based on nanotechnology materials and manufacturing processes developed by a company called Nanoident Technologies AG, formerly of Linz, Austria. The multimodal biometric sensor must be specially designed for use with the firearms to capture a number of biometric features including skin surface structure, subcutaneous tissue structure, and subcutaneous vein structure. It should be noted that Nanoident went insolvent in December 2008,[106] and the understanding is that Biomac has full contractual rights to use Nanoident technology. The Nanoident technology would need to be fully redeveloped in order to use this technology to layer the secondary sensors with the biometric sensor mentioned above.

## Online Resources

The following documents referenced in this report are publicly available and can be found online. The web addresses were accessed on May 31, 2013, and are current as of that date.

### The White House

Executive Office of the President, *Now Is The Time: The President's plan to protect our children and our communities by reducing gun violence*, January 16, 2013, http://wh.gov/now-is-the-time.

http://www.whitehouse.gov/sites/default/files/docs/wh_now_is_the_time_full.pdf

### Sandia National Laboratories

D.R. Weiss, *Smart Gun Technology Final Report*, Sandia Report SAND96-1131 (Albuquerque, NM: Sandia National Laboratories, 1996).

http://infoserve.sandia.gov/sand_doc/1996/961131.pdf

John W. Wirsbinski, *"Smart Gun" Technology Update*, Sandia Report SAND2001-3499 (Albuquerque, NM: Sandia National Laboratories, 2001).

http://infoserve.sandia.gov/sand_doc/2001/013499.pdf

### National Academy of Engineering

Lance A. Davis and Greg Pearson, editors, Steering Committee for NAE Workshop on User-Authorized Handguns, National Academy of Engineering, *Owner-Authorized Handguns: A Workshop Summary* (Washington, DC: National Academies Press, 2003).

http://www.nap.edu/catalog.php?record_id=10828

Committee on User-Authorized Handguns, National Academy of Engineering, *Technological Options for User-Authorized Handguns: A Technology-Readiness Assessment* (Washington, DC: National Academies Press, 2005).

http://www.nap.edu/catalog.php?record_id=11394

Committee on Radio Frequency Identification Technologies, National Research Council, *Radio Frequency Identification Technologies: A Workshop Summary*, (Washington, DC: National Academies Press, 2004).

http://www.nap.edu/catalog.php?record_id=11189

**National Institute of Justice**

List of awards made by NIJ:

http://nij.gov/nij/funding/awards/welcome.htm

**Office of Justice Programs**

OJP Grant Awards Advanced Search:

http://grants.ojp.usdoj.gov:85/selector/main

**Defense Technical Information Center**

Michael J. Feinberg, Geoge B. Niewenhous, and Marvin M. Maule, *Test Operations Procedure (TOP) 3-2-045 Small Arms - Hand and Shoulder Weapons and Machine Guns*, Small Arms Systems Division (CSTE-DTC-AT-FP-S), U.S. Army Aberdeen Test Center, September 17, 2007.

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA481861

A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The DET Curve in Assessment of Detection Task Performance," National Institute of Standards and Technology, 1997.

http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA530509

**Department of Defense**

Assistant Secretary of Defense for Research and Engineering, *Technology Readiness Assessment (TRA) Guidance*, Department of Defense, April 2011.

http://www.acq.osd.mil/ddre/publications/docs/TRA2011.pdf

## Glossary of Acronyms Used

| | |
|---|---|
| A | Amp |
| ANSI | American National Standards Institute |
| ARDEC | U.S. Army Armament Research, Development and Engineering Center |
| ATF | Bureau of Alcohol, Tobacco, Firearms and Explosives |
| ATM | Automated Teller Machine |
| BJA | Bureau of Justice Assistance |
| CFR | Code of Federal Regulations |
| CZ | Česká Zbrojovka |
| DET | Detection Error Tradeoff |
| DGR | Dynamic Grip Recognition |
| EP1 | Experimental Prototype 1 |
| EP2 | Experimental Prototype 2 |
| FAR | False Accept Rate |
| FBI | Federal Bureau of Investigation |
| FDA | Food and Drug Administration |
| FN | Fabrique Nationale |
| FR | Federal Register |
| FRR | False Reject Rate |
| ft | Foot |
| GmbH | Gesellschaft mit beschränkter Haftung |
| GPS | Global positioning system |
| HF | High Frequency |
| HTBL | Höhere Technische Bundeslehranstalten |
| IEEE | Institute of Electrical and Electronics Engineers |
| ISM | Industrial, Scientific, and Medical |

| | |
|---|---|
| JSSAP | Joint Service Small Arms Program |
| LED | Light-Emitting Diode |
| LLC | Limited Liability Company |
| m | Meter |
| mA | Milliamp |
| MEMS | Microelectromechanical System |
| MHz | Megahertz |
| MIL-SPEC | Defense Specification |
| mm | Millimeter |
| MP5 | Heckler & Koch MP5 |
| ms | Millisecond |
| NAE | National Academy of Engineering |
| NIJ | National Institute of Justice |
| NJIT | New Jersey Institute of Technology |
| NLECTC | National Law Enforcement and Corrections Technology Center |
| NSSF | National Shooting Sports Foundation |
| OEM | Original Equipment Manufacturer |
| OJP | Office of Justice Programs |
| PIN | Personal Identification Number |
| PLC | Programmable Logic Controller |
| RF | Radio Frequency |
| RFID | Radio Frequency Identification |
| ROC | Receiver-Operator Characteristic |
| R&D | Research and Development |
| SAAMI | Sporting Arms and Ammunition Manufacturers' Institute |
| SGR | Static Grip Recognition |

| | |
|---|---|
| SGT | Safe Gun Technology |
| SHOT | Shooting, Hunting, Outdoor Trade Show |
| SSBT | NIJ Sensors, Surveillance, and Biometrics Technologies Center of Excellence |
| SWS | Secure Weapon System |
| S&W | Smith & Wesson |
| TOP | Test Operations Procedure |
| TRA | Technology Readiness Assessment |
| TRL | Technology Readiness Level |
| UAHG | User-Authorized Handgun |
| USB | Universal Serial Bus |
| USTL | United States Test Laboratory |
| V | Volt |
| VLe | Variable Lethality |
| W | Watt |

## References

[1]Committee on User-Authorized Handguns, National Academy of Engineering, *Technological Options for User-Authorized Handguns: A Technology-Readiness Assessment* (Washington, DC: National Academies Press, 2005), 2. (hereafter cited in text as *NAE Tech. Options*).

[2]The White House, *Now Is The Time: The President's Plan to Protect Our Children and Our Communities by Reducing Gun Violence*, January 16, 2013, http://wh.gov/now-is-the-time.

[3]D.R. Weiss, *Smart Gun Technology Final Report*, Sandia Report SAND96-1131 (Albuquerque, NM: Sandia National Laboratories, 1996, hereafter cited in text as *Sandia Report*).

[4]John W. Wirsbinski, *"Smart Gun" Technology Update*, Sandia Report SAND2001-3499 (Albuquerque, NM: Sandia National Laboratories, 2001, hereafter cited in text as *Sandia Update*).

[5]Lance A. Davis and Greg Pearson, editors, Steering Committee for NAE Workshop on User-Authorized Handguns, National Academy of Engineering, *Owner-Authorized Handguns: A Workshop Summary* (Washington, DC: National Academies Press, 2003, hereafter cited in text as *NAE Workshop*).

[6]*NAE Tech. Options*.

[7]"Review of Gun Safety Technologies," 78 FR 11902 (February 20, 2013).

[8]*Sandia Report*.

[9]*Sandia Update*.

[10]*Sandia Report*.

[11]*Sandia Update*.

[12]*NAE Workshop*.

[13]*NAE Tech. Options*.

[14]*Sandia Report*, 34.

[15]Siegmund Halpern, *The Assurance Sciences: An Introduction to Quality Control and Reliability* (Englewood Cliffs, NJ: Prentice-Hall, 1978), 7 (hereafter cited in text as *Assurance Sciences*).

[16]*NAE Tech. Options*.

[17]Ibid.

[18]*Sandia Report,* section 2, "Requirements for a Smart Gun Technology," chapters 4 and 5, 27–61.

[19]Ibid., 34.

[20]The relevant passage is quoted here: "Let us examine more closely the term *reliability*. Dictionaries generally define reliable in terms of something that is trusty, authentic, consistent, and honest. When we speak of a *reliable product*, we usually expect such adjectives to apply. The problem with this manner of expressing the performance capability of a product is that it is very subjective. Different users may have different expectations as to a product's performance or life. There may also be a diversity of opinion as to what exactly constitutes degraded performance in contrast to failure.

"In the Assurance Sciences, the term *reliability* assumes a more definitive character: reliability may be defined, computed, tested, and verified. It may thus be specified in equipment procurement documents and contractually enforced. Most commonly, reliability is defined as *the probability that a device will perform its intended function for a specified period of time under stated conditions*. A probability of 99%, for example, means that on average a device will properly perform (as defined above) 99 of 100 times; or else that, on average, 99 or 100 devices will perform properly. Another well-known reliability measurement parameter is the MTBF (*mean time between failures*).

"The term *intended function* used to describe equipment performance makes it possible to identify what constitutes nonperformance of the equipment (i.e., failure).

"The specified period of time during which the equipment is to perform reliably may vary from the instantaneous operation of one-shot devices (e.g., explosive bolts) and operations lasting only a few hours to space missions lasting for years.

"The performance *under stated conditions* refers to the operational and environmental conditions, or stresses, that the equipment may experience during its required lifetime. Operational conditions vary from one piece of equipment to another, so it is important that the conditions are identified fully." *Assurance Sciences*, 7.

[21]Michael J. Feinberg, George B. Niewenhous, and Marvin M. Maule, *Test Operations Procedure (TOP) 3-2-045 Small Arms - Hand and Shoulder Weapons and Machine Guns*, Small Arms Systems Division (CSTE-DTC-AT-FP-S), U.S. Army Aberdeen Test Center, September 17, 2007.

[22]The American National Standards Institute (ANSI), the Sporting Arms and Ammunition Manufacturers' Institute (SAAMI), and the National Institute of Justice all have created standards related to firearms.

[23]Assistant Secretary of Defense for Research and Engineering, *Technology Readiness Assessment (TRA) Guidance*, Department of Defense, April 2011, section 2.5 (hereafter cited in text as *TRA Guidance*).

[24]iGun Technology Corporation, informational literature, March 2013.

[25]Ibid.

[26]*Assurance Sciences*, 7.

[27]Tom Fawcett, "ROC Graphs: Notes and Practical Considerations for Data Mining Researchers," *HP Labs Technical Reports*, HPL-2003-4 (Palo Alto, CA: Hewlett-Packard Company, 2003), accessed May 31, 2013, http://www.hpl.hp.com/techreports/2003/HPL-2003-4.pdf.

[28]A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, "The DET Curve in Assessment of Detection Task Performance," National Institute of Standards and Technology, 1997.

[29]Many resources are available on RFID technology, such as V. Daniel Hunt, Albert Puglia, and Mike Puglia, *RFID: A Guide to Radio Frequency Identification* (Hoboken, NJ: Wiley-Interscience, 2007); Klaus Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, trans. Dörte Müller (Chichester, West Sussex; Hoboken, NJ: Wiley, 2010); Committee on Radio Frequency Identification Technologies, National Research Council, *Radio Frequency Identification Technologies: A Workshop Summary* (Washington, DC: National Academies Press, 2004); *RFID Journal*, (Hauppauge, NY: RFID Journal LLC), http://www.rfidjournal.com.

[30]*NAE Tech. Options*, 7 and 35.

[31]See the "Technology Developers" section on FN Manufacturing in this report, page 31.

[32]See the "Technology Developers" section on iGun Technology Corporation in this report, page 29.

[33]See for example Anil K. Jain, Arun A. Ross, and Karthik Nandakumar, *Introduction to Biometrics* (New York: Springer, 2011), and references therein; "Introduction to Biometrics," Biometrics.gov, http://www.biometrics.gov/ReferenceRoom/Introduction.aspx; "Biometrics," National Institute of Justice, last modified September 15, 2011, http://nij.gov/biometrics.

[34]*TRA Guidance*.

[35]*NAE Tech. Options*, 18. In 1994, NIJ awarded $625,000 to Sandia National Laboratories in Albuquerque, NM.

[36]*Sandia Report*, section 2, "Requirements for a Smart Gun Technology," chapters 4 and 5, 27-61.

[37]*NAE Tech. Options*, 18. NIJ awarded an additional $70,000 to Sandia to update the 1996 report.

[38]*Sandia Update*.

[39]Lauren R. Taylor, "Getting Smarter: Making Guns Safer for Law Enforcement and Consumer," *National Institute of Justice Journal*, July 2000, https://www.ncjrs.gov/pdffiles1/jr000244d.pdf.

[40]National Law Enforcement and Corrections Technology Center, "Making Guns Smart: The Next Step," *TechBeat*, Winter 1999, https://www.justnet.org/InteractiveTechBeat/Winter-1999.pdf (hereafter cited in text as *TechBeat*).

[41]Colt's Manufacturing Company, Inc., *Smart Gun Development & Prototypes: Report #6; Final Report*, final report for award 97-LB-VX-K006 submitted to the National Institute of Justice, March 29, 2000.

[42]"NIJ Awards in Fiscal Year 1997," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/1997.htm. In 1997, NIJ provided $500,079 to Colt's Manufacturing Company, Inc. of Hartford, CT, under award 97-LB-VX-K006 over a 35-month period of performance.

[43]*TechBeat*.

[44]iGun Technology Corporation, accessed May 31, 2013, http://www.iguntech.com.

[45]iGun Technology Corporation, informational literature, March 2013.

[46]NIJ provided iGun with $3,000 to purchase the necessary ammunition for testing of the M-2000.

[47]iGun Technology Corporation, test report submitted to NIJ Office of Science and Technology, June 7, 2001.

[48]"NIJ Awards in Fiscal Year 2002," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2002.htm. In 2002, NIJ provided $299,389 to iGun Technology Corporation under award 2002-IJ-CX-K002.

[49]iGun Technology Corporation, *The Use of Biometrics to Control Access to a Personalized Law Enforcement Handgun*, final report for award 2002-IJ-CX-K002 submitted to the National Institute of Justice, December 2003.

[50]*NAE Tech. Options*, 5.

[51]NIJ provided a total of $3,082,477 to Smith & Wesson of Springfield, MA, under award 2000-RD-CX-K001, in two separate supplements over a nearly 44-month period of performance.

[52]"NIJ Awards in Fiscal Year 2000," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2000.htm. In 2000, NIJ provided $300,000 to Smith & Wesson under award 2000-RD-CX-K001.

[53]"OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2000, Program Office=NIJ, State/Territory=MA, Grant Type=All}, http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2000-RD-CX-K001&fiscalYear=2000&applicationNumber=2001-90201-MA-IJ&programOffice=NIJ&po=NIJ). In 2001, NIJ provided an additional $2,782,477 to Smith & Wesson under award 2000-RD-CX-K001.

[54]"NIJ Awards in Fiscal Year 2002," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2002.htm; "OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2002, Program Office=NIJ, State/Territory=MA, Grant Type=All}, http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2002-IJ-CX-K004&fiscalYear=2002&applicationNumber=2002-90311-MA-IJ&programOffice=NIJ&po=NIJ). In 2002, NIJ provided $590,884 to Smith & Wesson under award 2002-IJ-CX-K004 over a 36-month period of performance.

[55]Jeffrey Rankin, *Secure Weapon System (SWS) Smart Gun Technology, Phase I: Summary of Findings Report*, final report for award 2000-MU-MU-K005 submitted to the National Institute of Justice, July 2001, https://www.ncjrs.gov/pdffiles1/nij/grants/189247.pdf (hereafter cited in text as *SWS Phase I Report*).

[56]"NIJ Awards in Fiscal Year 2000," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2000.htm. In 2000, NIJ provided $300,000 to FN Manufacturing, Inc. of Columbia, SC, under award 2000-MU-MU-K005.

[57]*SWS Phase I Report*, 6-7.

[58]NIJ provided a total of $2,306,156 to FN Manufacturing under award 2001-IJ-CX-K017 in two separate supplements over a nearly 61-month period of performance.

[59]"NIJ Awards in Fiscal Year 2001," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2001.htm. In 2001, NIJ provided $1,271,826 to FN Manufacturing under award 2001-IJ-CX-K017.

[60]"NIJ Awards in Fiscal Year 2003," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2003.htm; "OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2001, Program Office=NIJ, State/Territory=SC, Grant Type=All}, http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2001-IJ-CX-K017&fiscalYear=2001&applicationNumber=2003-90304-SC-IJ&programOffice=NIJ&po=NIJ). In 2003, NIJ provided an additional $1,034,330 to FN Manufacturing under award 2001-IJ-CX-K017.

[61]BusinessWire, "VeriChip Corporation Enters into a Memorandum of Understanding for Development of a Firearm's User Authorization System — 'Smart Gun' — Using VeriChip RFID Technology," *BusinessWire*, April 13, 2004, http://www.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20040413005113&newsLang=en.

[62]*NAE Tech. Options*, 31.

[63]FN Manufacturing, Inc., *Summary of Findings Report: FN Secure Weapon System (SWS) Smart Gun Technology Phase IV*, final report for award 2001-IJ-CX-K017 submitted to the National Institute of Justice, September 6, 2006 (hereafter cited in text as *SWS Phase IV Report*).

[64]*SWS Phase IV Report*.

[65]*NAE Tech. Options*, 16.

[66]NIJ provided a total of $2,515,475 to NJIT under award 2004-IJ-CX-0096 in three separate supplements over a 43-month period of performance.

[67]"NIJ Awards in Fiscal Year 2004," National Institute of Justice, last modified November 28, 2007, http://nij.gov/nij/funding/awards/2004.htm. In 2004, NIJ provided $1,133,941 to NJIT under award under award 2004-IJ-CX-0096.

[68]"NIJ Awards in Fiscal Year 2005," National Institute of Justice, last modified November 30, 2007, http://nij.gov/nij/funding/awards/2005_topic.htm. In 2005, NIJ provided an additional $986,643 to NJIT under award under award 2004-IJ-CX-0096.

[69]"OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2006, Program Office=NIJ, State/Territory=NJ, Grant Type=Earmark}, http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2004-IJ-CX-0096&fiscalYear=2006&applicationNumber=2006-91962-NJ-IJ&programOffice=NIJ&po=NIJ). In 2006, NIJ provided an additional $394,891 to NJIT under award under award 2004-IJ-CX-0096.

[70]"OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2008, Program Office=BJA, State/Territory=NJ, Grant Type=Earmark}, http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2008-

DD-BX-0640&fiscalYear=2008&applicationNumber=2008-F4813-NJ-DD&programOffice=BJA&po=BJA). In 2008, BJA provided $254,889 to NJIT under award 2008-DD-BX-0640 over a 30-month period of performance.

[71]"OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2009, Program Office=BJA, State/Territory=NJ, Grant Type=Earmark}: http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2009-D1-BX-0210&fiscalYear=2009&applicationNumber=2009-H0795-NJ-DD&programOffice=BJA&po=BJA). In 2009, BJA provided $249,929 to NJIT under award 2009-D1-BX-0210 over a 22-month period of performance.

[72]"OCOM Award Index," Office of Justice Programs, http://grants.ojp.usdoj.gov:85/selector/main (OJP Grant Awards Advanced Search for {Fiscal Year=2010, Program Office=BJA, State/Territory=NJ, Grant Type=Earmark}, http://grants.ojp.usdoj.gov:85/selector/awardDetail?awardNumber=2010-DD-BX-K541&fiscalYear=2010&applicationNumber=2010-H8815-NJ-D1&programOffice=BJA&po=BJA). In 2010, BJA provided $1,000,000 to NJIT under award 2010-DD-BX-K541 over a 36-month period of performance.

[73]"NIJ Awards in Fiscal Year 2002," National Institute of Justice, last modified November 29, 2007, http://nij.gov/nij/funding/awards/2002.htm. In 2002, NIJ provided $185,000 to Metal Storm under award 2002-IJ-CX-K021.

[74]Metal Storm, *Advanced Smart Gun System for Law Enforcement Applications*, final report for award 2002-IJ-CX-K021 submitted to the National Institute of Justice, June 2003.

[75]J.A. Kauffman, A.M. Bazen, S.H. Gerez, and R.N.J. Veldhuis, "Grip-Pattern Recognition for Smart Guns," Paper presented at the 14th Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 26-27, 2003.

[76]Raymond N. Veldhuis, Asker M. Bazen, Joost A. Kauffman, and Pieter Hartel, "Biometric Verification Based on Grip-Pattern Recognition," *Proc. SPIE* 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 634, June 22, 2004.

[77]X. Shang, R.N.J. Veldhuis, A.M. Bazen, and W.P.T. Ganzevoort, "Algorithm Design for Grip-Pattern Verification in Smart Gun," Paper presented at the 16th Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 17-18, 2005.

[78]X. Shang and R.N.J. Veldhuis, "Registration of Hand-Grip Pattern in Smart Gun," Paper presented at the 17th Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 23-24, 2006.

[79]Xioaxin Shang and R. Veldhuis, "Local Absolute Binary Patterns as Image Preprocessing for Grip-Pattern Recognition in Smart Gun," Paper presented at the IEEE First International Conference on Biometrics: Theory, Applications, and Systems, 2007.

[80]Xioaxin Shang and R. Veldhuis, "Grip-Pattern Verification for Smart Gun Based on Maximum-Pairwise Comparison and Mean-Template Comparison," Paper presented at the IEEE Second International Conference on Biometrics: Theory, Applications, and Systems, 2008.

[81]Xioaxin Shang and Raymond N.J. Veldhuis, "Grip-Pattern Recognition in Smart Gun Based on Likelihood-Ratio Classifier and Support Vector Machine," in *Image and Signal Processing*, ed. A. Elmoataz, O. Lezoray, O., F. Nouboud, and D. Mammass, Proceedings of the 3rd International Conference, ICISP 2008, Cherbourg-Octeville, France, July 1-3, 2008 (Berlin: Springer, 2008), 289-295.

[82]Xioaxin Shang, "Grip Pattern Recognition Applied to a Smart Gun" (Ph.D. dissertation, University of Twente, December 19, 2008), http://eprints.eemcs.utwente.nl/14292/01/ThesisShangFinal.pdf.

[83]"Smart System," Armatix GmbH, accessed May 31, 2013, http://www.armatix.us/Smart-System.778.0.html?&L=7.

[84]"iW1active RFID watch," Armatix GmbH, accessed May 31, 2013, http://www.armatix.us/iW1-active-RFID-watch.780.0.html?&L=7.

[85]"iP1Pistol," Armatix GmbH, accessed May 31, 2013, http://www.armatix.us/iP1-Pistol.779.0.html?&L=7.

[86]Armatix GmbH, *iP1 SmartSystem Quick Start Guide*.

[87]"OET List Exhibits Report," Office of Engineering and Technology, Federal Communications Commission, https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&calledFromFrame=Y&application_id=740871&fcc_id=ZYXSMARTIP1.

[88]"OET List Exhibits Report," Office of Engineering and Technology, Federal Communications Commission, https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&calledFromFrame=Y&application_id=905854&fcc_id=ZYXSMARTIW1.

[89]Letter from John R. Spencer, Chief, Firearms Technology Branch, to The Sportsman's Shop, December 22, 2011, 2012-198-MSK.

[90]United States Test Laboratory, Revised California Compliance Test Report on Armatix GmbH Model IP1, .22 LR, 3.58" Barrel, January 24, 2013.

[91]California Penal Code, Section 31900-31910, http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=31001-32000&file=31900-31910.

[92]"Roster of Handguns Certified for Sale," Office of the Attorney General, State of California Department of Justice, accessed May 31, 2013, http://certguns.doj.ca.gov.

[93]"Roster of Firearm Safety Devices Certified for Sale," Office of the Attorney General, State of California Department of Justice, accessed May 31, 2013, http://oag.ca.gov/firearms/fsdcertlist.

[94]Aaron Rowe, "High-Tech Guns: Digital Revolvers, Koosh Bullets and Triple-Tasers," *Wired*, posted January 28, 2010, http://www.wired.com/dangerroom/2010/01/high-tech-guns-digital-revolvers-koosh-bullets-and-triple-tasers/all/.

[95]"SHOT Show," National Shooting Sports Foundation, accessed May 31, 2013, http://www.nssf.org/SHOT/.

[96]Safe Gun Technology, informational literature, January 2013.

[97]TriggerSmart Technologies, accessed May 31, 2013, http://www.triggersmart.com.

[98]TriggerSmart, informational literature, January 2013.

[99]X. Qing and Z.N. Chen, "Proximity effects of metallic environments on high frequency RFID reader antenna: study and application," *IEEE Trans. on Antennas and Propagation*, Vol. 55, No. 11, 3105-3111, November 2007.

[100]X. Qing and Z.N. Chen, "Characteristics of a metal-backed loop antenna and its application to a high-frequency RFID smart shelf," *IEEE Antennas and Propagation Magazine*, Vol. 51, No. 2, 26-38, April 2009.

[101]TriggerSmart, informational literature, January 2013.

[102]Robert J. Kosinski, "A Literature Review on Reaction Time," last updated September 2012, http://biae.clemson.edu/bpc/bp/Lab/110/reaction.htm.

[103]Intelligun, accessed May 31, 2013, http://www.intelligun.com.

[104]Biomac Systems, Inc., Business Plan Summary, May 2012.

[105]Ibid.

[106]"Company Overview of Nanoident Technologies AG," *Businessweek*, accessed May 31, 2013, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=24953128.

The National Institute of Justice is the research, development and evaluation agency of the U.S. Department of Justice. NIJ's mission is to advance scientific research, development and evaluation to enhance the administration of justice and public safety.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance; the Bureau of Justice Statistics; the Office for Victims of Crime; the Office of Juvenile Justice and Delinquency Prevention; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART).

U.S. Department of Justice
Office of Justice Programs
*National Institute of Justice*

Washington, DC 20531

Official Business
Penalty for Private Use $300

PRESORTED STANDARD
POSTAGE & FEES PAID
DOJ/NIJ
PERMIT NO. G-91

NCJ 242500