Report to the President Outlining a Strategy to Expedite Deployment of Gun Safety Technology

Submitted by the
Departments of Justice, Homeland Security, and Defense

April 2016

Introduction

For more than two decades, the federal government and the private sector have grappled with a basic question of firearm engineering: Can modern technology make guns safer—or "smarter"—without sacrificing the reliability, durability, and accuracy that owners expect from their firearms?

The technology holds great promise. By incorporating electronic systems into a firearm's design, manufacturers can give gun owners greater control over how a weapon is used, both by limiting who can fire the gun ("user-authorization technology") and by making a gun easier to retrieve if it is lost or stolen ("electronic recovery technology"). As noted in the President's January 4, 2016, Memorandum on Promoting Smart Gun Technology, these innovations have the potential to reduce accidental and unauthorized firearm discharges, in turn making our country and its citizens safer. To achieve these changes, the federal government must develop a research and development strategy to expedite real-world deployment of such technology for use in practice.

Much of the basic technology exists. As President Obama said in his remarks accompanying the release of the January 2016 Memorandum, if "you can't unlock your phone unless you've got the right fingerprint, why can't we do the same thing for our guns? If there's an app that can help us find a missing . . . iPad, there's no reason we can't do it with a stolen gun." The President is right. Consumers have grown accustomed to technological advances, such as fingerprint readers and near-field communication, that are common in other industries but virtually nonexistent in firearms manufacturing.

But the next step is more challenging. Manufacturers must now find ways to effectively integrate this technology into firearms without compromising the core functions of the device. Gun owners—whether law enforcement officers, hunters, or homeowners seeking to protect their property—expect their firearms to work seamlessly, under all conditions, without concern for technical malfunction. To make "smart" gun technology saleable to a wide range of consumers, manufacturers must ensure that these firearms operate properly in the high-stress situations when firearms are needed most.

Numerous industries have found ways to integrate modern electronics into older mechanical systems without undermining the quality of the product. In automobiles, for example, owners rely on a range of computerized systems—from anti-lock brakes to airbags—that operate instantly and provide far greater protection to drivers than earlier, less sophisticated systems. Such advancements have been possible due to sustained investment by private companies—and, at times, support and direction from government actors.

Firearms manufacturers will need to decide whether to make similar investments here. To achieve the innovations that the President seeks, one or more companies must

decide that the benefits of enhanced gun safety technology exceed the costs of researching, developing, and marketing such technology.

Federal, state, and local governments can support this effort in two ways: by lowering the cost of bringing new technology to market, and by exercising their collective purchasing power, where appropriate, to spur development. This report proposes a policy initiative that would support both of these methods. Over the next six months, the Administration will partner with state, county, and municipal law enforcement agencies to establish the specific conditions under which they would consider purchasing firearms with advanced gun safety technology.

This partnership will result in the drafting of voluntary "baseline specifications" that will outline—for the first time—a clear description of what law enforcement expects from smart gun technology, particularly with regards to reliability, durability, and accuracy. These baseline specifications will serve several purposes. First, they will provide clear guidance to potential manufacturers about what government purchasers require in their firearms. Second, these specifications will serve as a standard against which existing technology can be measured, making it possible to identify what research and development gaps remain. And finally, this process will allow federal, state, and local governments to demonstrate that demand for these weapons may exist—if certain operational requirements are met.

We expect that these specifications will be demanding. Law enforcement agencies cannot and should not equip their officers with firearms that make them, or the communities they serve, less safe. But by inviting law enforcement professionals to develop specifications, the Administration can lay the groundwork for expanded use of gun safety technology in the near future. Most importantly, this process will leverage the government's procurement power to encourage the type of entrepreneurial, market-driven innovation that undergirds the American economy, thus maximizing the government's impact at a time when federal research funds are scarce.

To be clear, this report calls for the development of new technology—and not a mandate that any particular individual or law enforcement agency adopt the technology once developed. By spurring the growth of enhanced gun safety technology, the federal government seeks to expand, not constrict, consumers' choices when deciding what firearm to purchase. Over time, as the technology improves, consumers may grow to prefer these new safety features, and state and local law enforcement agencies may decide to use their federal grant funds to purchase firearms equipped with such technology. Here, as in many other industries, the government can serve as a market participant, encouraging important technological advancements with the potential to benefit both law enforcement officers and the public at large.

User-Authorization Technology

In 1996, the federal government published its first significant report on advanced gun safety technology—the culmination of a multi-year partnership between the National Institute of Justice (NIJ), which serves as the research, development, and evaluation agency of the Department of Justice (DOJ); and Sandia National Laboratories (Sandia), a research center operated by the Department of Energy.[1] The project concentrated on the viability of user-authorization "smart gun" technology, with a particular focus on whether the technology could reduce the risk of so-called firearm "takeaways"—i.e., when a suspect seizes an officer's weapon during a law enforcement operation. The 1996 Sandia report concluded that user-authorization technology could limit this risk, but that significant additional research and development was required before this technology could be effectively integrated into the types of firearms most commonly used by law enforcement. Since then, NIJ has funded a number of additional projects to further the development of this technology, with progress advancing intermittently over the past two decades.

A. Potential Benefits of User-Authorization Technology

Before reviewing the successes and limitations of existing technology, it is helpful to consider why this technology could be useful for law enforcement agencies. If fully developed, these technological advancements could create safer firearms, limiting their use to the officers trained to handle them. This report identifies several possible benefits:

- *Limiting "takeaways" during law enforcement operations.* As discussed in the 1996 Sandia report, user-authorization technology could limit the ability of a suspect to seize a firearm from an officer during a law enforcement operation and use it against him or her. Although these "takeaway" killings occurred in a variety of circumstances, the report indicated that they were most common along a roadway after a traffic stop, and typically involved a struggle before the adversary attempted to escape.

- *Limiting misuse of lost and stolen law enforcement firearms.* User-authorization technology could also reduce the risk of misuse when an officer's service weapon has been lost or stolen. Nationwide, the theft and loss of firearms remains a serious problem. In 2012, for example, the FBI's National Crime Information Center received reports of nearly 200,000 lost or stolen firearms in the country, although it is unknown exactly how many of these weapons were owned by law

[1] D.R. Weiss, Smart Gun Technology Project Final Report, Sandia National Laboratories (May 1996), available at http://prod.sandia.gov/techlib/access-control.cgi/1996/961131.pdf.

enforcement.[2] Advanced gun safety technology would prevent use of an officer's weapon if it fell into the wrong hands—and might discourage theft of such weapons in the first place. These developments could, in turn, shrink the supply of stolen firearms to the secondary black market, curtailing a dangerous source of weapons for criminals.

- *Limiting accidental off-duty discharges by officers' children and other family members.* User-authorization technology would also limit the likelihood that an officer's family members accidentally discharge his or her service weapon inside the home. When off-duty, many law enforcement officers store their service weapons inside their residences—and, as with any gun inside the home, there is a risk of accidental discharge, even when the firearm is safely secured. Although it is unknown how often an officer's weapon is mishandled by a child or other family member, there are reports of accidental shootings and deaths.[3]

Needless to say, user-authorization technology will not necessarily eliminate all unauthorized use of firearms, nor is this technology the only solution to accidental and improper firearm use. (Among other things, law enforcement agencies routinely train their officers on how to mitigate the risks described above, including through trainings on the proper use and storage of their service weapons.) But this technology, if fully developed, could further enhance the safety of law enforcement officers and those who interact with them and could help ensure that government-issued firearms are used only for their intended purposes.[4]

B. Promoting Technological Development

Since the 1996 Sandia report, the federal government and private manufacturers have sought to create several variations of user-authorization technology. Broadly speaking,

---

[2] Bureau of Alcohol, Tobacco, Firearms, and Explosives, 2012 Summary: Firearms Reported Lost and Stolen (June 2013), available at https://www.atf.gov/resource-center/docs/2012-firearms-reported-lost-and-stolenpdf-1/download.

[3] Sadie Gurman, "Police Cope with Keeping Guns Secured Safely at Home," *Pittsburg Post-Gazette,* December 6, 2010, available at http://www.post-gazette.com/local/region/2010/12/06/Police-cope-with-keeping-guns-secured-safely-at-home/stories/201012060280.

[4] Over the long term, there could be additional public safety benefits associated with the development of user-authorization technology. For example, to the extent that members of the general public also decide to purchase firearms equipped with such technology, there may be a broader reduction in the number of accidental or unauthorized discharges of firearms nationwide, potentially resulting in fewer injuries and deaths.

firearm developers have pursued two methods for user authentication: biometric readers, such as fingerprint or palmprint sensors, that are built into the grip of the gun; and proximity devices, typically involving radio frequency identification (RFID) tags, that are embedded in a wristband, ring, or badge worn by the user. Some of these efforts have involved the design of an entirely new firearm, with the user-authentication technology integrated into the system design from the beginning, while other efforts have involved the development of add-on devices and other accessories that could be retrofitted onto existing firearms.

These efforts have shown mixed results. Over the past two decades, a number of promising designs have emerged, although many of these projects were suspended or cancelled before a final product could be completed. Although the reasons for terminating these projects have varied, there has been a consistent theme: the difficulty of integrating new technology into a firearm's design without compromising its core functions. Generally speaking, additional complexity brings increased risk of malfunction and error. The types of firearms most commonly used by law enforcement and the broader American public, whether rifles, revolvers, or semi-automatic pistols, are relatively straightforward mechanical devices, and manufacturers have faced significant engineering challenges as they seek to seamlessly integrate electronics into firearms' operations.

In January 2013, President Obama directed DOJ to review existing and emerging gun safety technologies and then issue a report on their availability and potential use. Over the following six months, NIJ engineers and analysts conducted an assessment of user-authorization technology, including through site visits, interviews, and literature reviews. This work culminated in the June 2013 publication of *NIJ Research Report: A Review of Gun Safety Technologies*, which summarized the federal government's history of financial support for user-authorization technology and described the various efforts by private manufacturers to develop this technology for commercial use.

The 2013 NIJ report noted that DOJ has issued at least $12.6 million in grants to support this technology over the previous two decades. Most of the funding—approximately $11.1 million—was provided by NIJ itself, as part of a broader effort to spur research and standards development for technologies that would benefit law enforcement operations, including advancements in firearms, body armor, and communications devices. An additional $1.5 million in funding was provided by the Bureau of Justice Assistance (BJA), housed within DOJ's Office of Justice Programs.

The DOJ grants are summarized below:

- *Colt's Manufacturing Co., 1997-2000 ($500,079).* In 1997, NIJ awarded approximately half a million dollars to Colt's Manufacturing to develop a firearm that would be locked by an RFID wristband worn by the user. The company

delivered two prototypes in 2000, although they were deemed too unreliable to undergo substantial test firings.

- *Smith & Wesson, 2000-2005 ($3,673,361).* Beginning in 2000, NIJ awarded approximately $3.67 million to Smith & Wesson, which explored several types of firearm authentication, including PIN codes, fingerprint sensors, and skin tissue spectroscopy. Although the company originally planned to deliver 50 prototypes for testing and evaluation, only two were ultimately delivered. The project ended in 2005.

- *FN Manufacturing, Inc., 2000-2006 ($3,606,156).* Beginning in 2000, NIJ awarded approximately $2.6 million to FN Manufacturing to develop a firearm, known as the "Secure Weapon System," that would be unlocked by an RFID device worn as a ring on the user's firing hand. FN Manufacturing ultimately delivered three prototypes of the handgun. During testing, the prototypes fired a combined 1,500 rounds with only one mechanical incident, although evaluators noted that the weapon behaved erratically and that blunt force could override the authentication system. The grant funding ended in 2006 and FN Manufacturing did not pursue the project further.

- *Five NIJ awardees, 2002 ($1,147,353, combined).* In 2002, NIJ awarded small grants to five manufacturers to explore different user-authorization technologies: Mosermation; Technology Next; VLe Small Arms; Exponent; and iGun Technology. The most advanced of these efforts involved iGun Technology, which had previously developed a shotgun in 1999 that could be unlocked by an RFID device worn as a ring on the user's firing hand.

- *New Jersey Institute of Technology, 2004-2014 ($4,020,293).* Starting in 2004, NIJ awarded a grant to New Jersey Institute of Technology (NJIT) to develop a firearm unlocked by "dynamic grip recognition," which involved multiple pressure sensors located on the left and right grip pads on the handle. In 2008, the source of the funding transferred from NIJ to BJA, which continued to support the initiative until all program funding was expended in 2014.

The 2013 NIJ Report also included a summary of all major past and current efforts by private manufacturers to develop user-authorization technology. The report identified thirteen projects in total, some of which had been government-funded, and some of which had not been. The NIJ report then divided these thirteen projects into three categories—"upper," "middle," and "lower"—based on the maturity of the technology developed. The report concluded that three of the thirteen products qualified for the "upper" tier, signaling

that they were ready, or nearly ready, for commercial production. Those three "commercializable" firearms were:

- *Armatix "Smart System" (.22 caliber pistol, with RFID wristband).* Developed by the German-based Armatix, a spinoff of SimonsVoss AG, the "Smart System" is arguably the most technologically mature user-authorization firearm ever developed. To unlock the firearm, the user enters a five-digit PIN code into a specialized wristband, which then allows the .22 caliber pistol, called the "iP1," to be used for determinate period of time (between one and eight hours). The firing mechanism becomes inoperable if the pistol is moved more than 15 inches from the wristband. In 2011, ATF approved the iP1 pistol for importation into the United States, and the firearm is currently approved for sale in California and Massachusetts.

- *Kodiak "Intelligun" (add-on fingerprint sensor, designed for .45 caliber model 1911-style pistol).* In 2012, Utah-based Kodiak Industries launched the "Intelligun," a fingerprint-based locking system that can be installed on a .45 caliber model 1911-style handgun. To unlock the firearm, the user grips the handle, then places his or her middle finger on a biometric sensor installed on the grip; once activated, the user can continue firing the weapon until he or she releases the handle. Kodiak reported that the device unlocks in a fraction of a second, and that the sensor can store the fingerprints of multiple users. The entire system weighs less than one round of ammunition and includes a battery designed to last approximately 800 hours of use. Kodiak also reported that it expects the failure rate of the device to be less than 1-in-10,000.

- *iGun Technology "M-2000" (12-gauge shotgun, with RFID ring).* In 1998, Florida-based iGun Technology developed the M-2000 shotgun, possibly the first ever production-ready firearm equipped with user-authorization technology. The user unlocks the firearm by wearing an RFID ring, which allows the weapon to fire as long as the ring is within two inches of the stock of the gun. The device unlocks in less than a quarter of a second, can be configured to work with multiple RFID rings, and includes a battery designed to work for 10 years. Several years after developing the M-2000, iGun partnered with West Virginia University and obtained a NIJ grant (as noted above) to study whether biometric features could be incorporated into the device. Although the M-2000 was never available for commercial sale, the company estimates that it produced enough components in 1998 to assemble 50 working units if ordered by a buyer.

Notably, none of the three products deemed "commercializable" in the 2013 NIJ report were developed using government funds. Armatix's Smart System, Kodiak's Intelligun, and iGun's M-2000 were all produced by private manufacturers that invested significant resources into research and development. (iGun later sought NIJ funding, but this money was not used in the original development of the M-2000.)

Since the release of the 2013 NIJ report, a number of additional manufacturers, inventors, and entrepreneurs have joined the effort to develop user-authorization technology. In 2014, the Smart Tech Challenges Foundation, based in Silicon Valley, issued a $1 million challenge to fund innovative new technologies.[5] Since then, Smart Tech has provided start-up capital to a number of promising companies and individuals developing new gun safety devices, including a high school senior whose fingerprint-based pistol earned one of the top awards at the 2013 Intel International Science and Engineering Fair. The effort received a further boost when San Francisco Police Chief Greg Suhr announced that he would allow his officers to participate in a pilot project to test user-authorization firearms once the technology matures further.[6]

NIJ continues to evaluate promising gun safety technologies. As noted below, the federal government anticipates additional research and development efforts in future years, and NIJ has committed to considering new research projects in Fiscal Year 2017 and beyond as part of a broader strategy to develop baseline specifications for law enforcement use.

C. DOJ's Ongoing Gun Safety Technology Challenge

In January 2013, alongside his directive to DOJ, President Obama announced that the Administration would "issue a challenge" to the private sector to encourage the development of innovative and cost-effective gun safety technology. This announcement resulted in the "Gun Safety Technology Challenge," unveiled by NIJ in October 2015. NIJ structured the Challenge as a three-stage test to evaluate the reliability and durability of firearms equipped with user-authorization technology. Under the Challenge rules, firearms manufacturers would submit their products for rigorous testing by NIJ and the U.S. Army Aberdeen Test Center (ATC), and then would receive small cash prizes if their products passed the second and third stages of the evaluation. More important than the cash rewards,

---

[5] Benny Evangelista, "Tech Foundation Challenges Innovators to Find Gun Safety Fix," *S.F. Chronicle*, January 28, 2014, available at http://www.sfgate.com/business/article/Tech-foundation-challenges-innovators-to-find-gun-5183207.php.

[6] Benny Evangelista, "Smart Gun Industry May Have Found its Test Bed – San Francisco," *S.F. Chronicle*, February 24, 2016, available at http://www.sfgate.com/business/article/Smart-gun-industry-may-have-found-its-test-bed-6850142.php.

however, was the opportunity for firearms manufacturers to demonstrate that their products operated under harsh, real-world conditions—an essential step in convincing potential customers of their long-term value.

Over the past several months, NIJ has been accepting and reviewing submissions as part of Stage 1, and two manufacturers were ultimately invited to advance to Stage 2: Armatix and Protobench, LLC. On February 17, 2016, NIJ and ATC met with the Department of Homeland Security's (DHS) Science & Technology Directorate (S&T) to discuss next steps in the Challenge. The release of this report marks the opening of Stage 2.

The three stages of the Challenge are described below:

- *Stage 1: Information and Safety Review.* The first stage of the Challenge involved an information review. Participants submitted a white paper describing their product or technology, along with any existing test reports relating to performance or reliability. The submitted material was reviewed and evaluated by NIJ and ATC to determine whether the product is eligible for Stage 2. During this process, more than a dozen manufacturers delivered submissions; however, many of the white papers described prototypes or other proposals not yet ready for real-world testing. As noted above, two manufacturers were invited to advance to Stage 2: Armatix and Protobench, LLC.

- *Stage 2: Light-Duty, Single Product Testing.* The second stage of the Challenge, which begins with the release of this report, will involve light-duty testing. Participants will be asked to submit firearms or firearm accessories for testing at the Aberdeen Proving Ground. Evaluations of test data will employ "failure definition and scoring criteria" (FDSC) developed in accordance with established guidelines already in use for reliability testing in the U.S. Army. A review panel of subject-matter experts will inspect the test results and assess the performance of entries based on the FDSC used to characterize failures. Manufacturers that pass Stage 2 will be entitled to a $5,000 cash prize.

- *Stage 3: Heavy-Duty, Expanded Product Testing.* During the third stage of the Challenge, NIJ and ATC will conduct heavy-duty testing of multiple products. Participants will be expected to submit multiple firearms, which will be subjected to extensive firing tests, as well as additional environmental evaluations designed to test functionality and durability under different conditions. Stage 3 will also involve testing to determine the vulnerability of the firearm technology, such as electromagnetic inference testing. Manufacturers that pass Stage 3 will be entitled to a $10,000 cash prize.

Additional information regarding the Challenge can be found on NIJ's website.[7] NIJ will periodically update the website during the Challenge, including with details regarding the progress of Stages 2 and 3.

Electronic Recovery Technology

In recent years, another type of gun safety technology has emerged: real-time data collection involving the location and use of law enforcement firearms. Although the effort is still in its infancy, several manufacturers have developed products that might warrant further study.

The technology is relatively straightforward: a computer chip, embedded in a law enforcement firearm, that transmits information about its location and use. In its simplest form, the chip can provide real-time location data, making it easier for officers to recover a weapon if it has been lost or stolen. More sophisticated systems can collect additional information about the gun's use—such as when the weapon has been unholstered or discharged—and can use this data to automatically notify police dispatchers when an officer requires back-up.

Unlike user-authorization technology, this type of real-time data collection does not affect the mechanical operation of the firearm, though it does require police departments to develop the networking infrastructure to process the data. Several manufacturers have developed products that are being tested in pilot projects:

- *Beretta "i-PROTECT" System.* The Italian manufacturer Beretta is currently testing its i-PROTECT system, which integrates motion sensors into its Px4 Storm pistol. The sensors are triggered when the firearm is drawn from its holster, when the hammer is armed or disarmed, and when the gun is fired. The data is then transmitted to the officer's smartphone, which then passes the information to a police operations center.[8]

- *Yardarm Sensor.* The California-based Yardarm Technologies has developed its own sensor, which includes a programmable microcontroller, magnetometer, accelerometer, and gyroscope. The data is fed to a Bluetooth transmitter paired with the officer's smartphone, which is then transmitted via encrypted network to a police operations center. In 2014, Yardarm announced that it had partnered

[7] "Gun Safety Technology Challenge," National Institute of Justice, http://www.nij.gov/funding/pages/fy16-gun-safety-challenge.aspx

[8] "i-Protect," Beretta, http://www.beretta.com/en/world-of-beretta/beretta-news/new-products-i-protect-july-2015/

with local police departments in California and Texas to test the technology in a pilot project.[9]

To date, NIJ has not funded any research or evaluation of this technology. As these products develop, however, it may be appropriate for NIJ and other federal agencies to examine methods for establishing standards for use and provide guidance to law enforcement agencies considering this technology.

Strategy to Develop Baseline Specifications for Law Enforcement Use

As President Obama made clear, the federal government can and should support efforts to advance technology that enhances gun safety and improves law enforcement operations. If fully developed, these technologies could reduce accidental or improper uses of law enforcement firearms, in turn saving lives and strengthening public safety. All law enforcement agencies—federal, state, and municipal—stand to benefit from these efforts.

It is clear, however, that additional work is required before this technology—both user-authorization and electronic-recovery technology—is ready for widespread adoption by law enforcement agencies. The government nonetheless can play an important role in furthering this work. As significant purchasers of firearms, federal, state, and local law enforcement agencies can use their combined purchasing power, where appropriate, to spur additional development and help establish a robust market for firearms equipped with this technology.

As a first step, however, law enforcement agencies must clearly define under what conditions they would consider purchasing firearms with this advanced technology. By developing "baseline specifications," federal, state, and municipal law enforcement agencies can make clear to private manufacturers what they expect from this technology, which in turn will make it possible to determine what additional research or development is required.

A. Timeline of Development Process

This report outlines a multi-stage approach for developing these baseline specifications. From beginning to end, this process should focus on the operational needs of law enforcement—with a clear understanding that law enforcement agencies can and should only procure firearms and other products that actually meet the needs of the agencies and their employees. In addition, it is crucial that these baseline specifications are developed

[9] Caleb Garling, "Police in California and Texas Test Networked Guns," MIT Technology Review, November 13, 2014, available at https://www.technologyreview.com/s/532426/police-in-california-and-texas-test-networked-guns.

in collaboration with state and local law enforcement, recognizing that these agencies represent a far greater share of law enforcement personnel than their federal counterparts.

A multi-stage plan is outlined below:

- *Step 1: Experts in firearms technology prepare draft list of specifications.* As a first step, the federal government will assemble a team of experts in firearms technology to prepare a draft list of baseline specifications. Starting in April 2016, DOJ and DHS will convene a working group, led by NIJ and comprised of representatives from federal law enforcement agencies, to identify operational needs. As part of this process, the working group will engage with firearms experts at state and local law enforcement agencies, and will consult with other relevant stakeholders, such as firearms manufacturers. (This work will also build on an effort, already underway within DHS, to determine basic common requirements.[10]) The working group intends to complete draft specifications by July 15, 2016.

- *Step 2: Convening of law enforcement agencies.* In mid-August 2016, DOJ and DHS will convene federal, state, and local law enforcement agencies for a one-day session to review and discuss the draft specifications prepared by the interagency working group. Based on this feedback, the working group will revise the specifications as appropriate and finalize the document for publication. The working group intends to incorporate revisions and prepare a final version of baseline specifications by October 15, 2016.

- *Step 3: Voluntary commitments by law enforcement agencies.* In autumn 2016, once the baseline specifications have been published, participating law enforcement agencies will be invited to make voluntary commitments regarding the development and procurement of this technology. Agencies will be asked to determine what, if any, steps they would be willing to take—if and when one or more manufacturers succeed in developing a product that meets these specifications. These voluntary commitments could include:

[10] In February 2016, for example, DHS S&T held a kickoff meeting with representatives from Federal Law Enforcement Training Centers (FLETC), Federal Emergency Management Agency (FEMA), United States Coast Guard (USCG), Customs and Border Patrol (CBP), National Protection and Programs Directorate/Federal Protective Service (NPPD/FPS), Immigration and Customs Enforcement (ICE), United States Secret Service (USSS), Office of Law Enforcement Policy, and the Military Advisor to the DHS Secretary to begin the process of determining common requirements. It is anticipated that this effort will strengthen and support the DOJ-DHS Working Group outlined in this report.

- *Commit to conduct officer pilot program.* An agency could agree to procure a small number of firearms equipped with advanced gun safety technology as part of a pilot program with a select group of law enforcement officers.
- *Commit to add firearm to approved purchase list.* Some law enforcement agencies allow officers to select their preferred service weapon from a list of approved firearms manufacturers. An agency could agree to add a firearm equipped with advanced gun safety technology to the list of approved service weapons, which would allow officers to decide for themselves whether they wished to use the new technology while on patrol.

- *Step 4: Identification of remaining gaps.* Once the baseline specifications have been finalized, the federal government can and should work with private industry to identify the most substantial research and development gaps between existing technology and law enforcement specifications. As part of this effort, NIJ commits to considering additional research projects, supported by funds available in Fiscal Year 2017 and beyond, that would close these gaps.

Taken together, these steps will advance the President's goals and leverage the expertise of federal firearms specialists to encourage further development of gun safety technology.

B. Federal Grants for State and Local Law Enforcement

The framework described above lays the foundation for law enforcement agencies to begin purchasing smart guns when the technology is ready for widespread use. The federal government stands ready to assist state and local governments as these devices enter the commercial market. Over the past four years, for example, BJA has distributed more than $1 billion to state and local governments through the Edward Byrne Memorial Justice Assistance Grant (JAG) program, which provides formula-based and discretionary funds to support criminal justice projects, including the purchase of law enforcement equipment. DOJ anticipates that as new firearms—including those equipped with smart gun technology—become available, state and local governments could apply JAG funds to the purchase of such devices. By helping to defray these costs, the federal government can make it possible for law enforcement agencies to obtain new technology that enhances the safety of their officers and the broader public.

As the Administration undertakes the effort of drafting baseline specifications, BJA, NIJ, and other federal entities will seek ways to highlight the availability of federal grant funding to support the purchase of firearms and related equipment for law enforcement use. By educating manufacturers and developers about these funds, the Administration can help to demonstrate the size of the potential market for advanced gun safety technology, creating

further incentives for private industry to continue their ongoing research and development efforts.

C. Identifying Issues for Baseline Specifications

The process described above will result in the development of baseline specifications for law enforcement adoption of advanced gun safety technology. This report identifies several potential issues that law enforcement agencies will likely consider as they develop these specifications:

- *Reliability.* The most important aspect of advanced gun safety technology is that the entire system be reliable. As a result, any new technology should not reduce the reliability of the firearm system, as compared to existing firearms. In the rare cases when the technology does fail, officers should have some way of operating the firearm when confronted with an adversary.

- *Durability.* Law enforcement officers expect their firearms to work in all conceivable circumstances and environments, including extreme weather conditions and when exposed to various contaminants, such as dirt or blood. New gun safety technology should not reduce the circumstances in which the firearm will operate, as compared to existing firearms.

- *Permitting multiple users.* From time to time, an officer will need to use another officer's firearm—for example, because the firearm has failed, or because the officer is incapacitated. In addition, some firearms, such as service shotguns, are routinely used by multiple members of the same patrol unit. As a result, it is important that user-authorization technology allows multiple individuals to use a firearm, including an officer's partner and other members of the patrol unit, and that the technology allows for up- and down-scaling (i.e., increasing or decreasing the number and identities of authorized persons) easily and reliably.

- *Physical characteristics of firearm.* Officers have grown accustomed to the appearance and characteristics of their service weapons. Ideally, a firearm equipped with user-authentication technology should physically look like existing firearms, and be recognizable to other officers and suspects. In addition, the technology should not appreciably change the weight, size, or balance of existing firearms, or increase the likelihood that the weapon would snag when drawn from an officer's holster.

- *Ease and predictability of use.* An officer must be able to activate the technology without assistance from others, and it should be easy for an officer to determine whether the device is working. The system should have both a very low false-

rejection rate (when an authorized user is incorrectly blocked from using the gun) and a very low false-acceptance rate (when an unauthorized user is allowed to fire the weapon). In addition, an officer should be able to use the firearm while wearing gloves.

- *Cost.* Most law enforcement budgets devote only a small percentage of their budget to purchasing equipment, and many departments are unable to supply or update their existing equipment with the latest technologies. In some jurisdictions, officers have to purchase their own service firearms. While some officers may be willing to pay a premium for the peace of mind of owning a gun with advanced gun safety technology, others may not.

- *Training.* It should be easy to train officers and armorers on user-authorization technology, and the costs of the additional training to police departments should be minimal.

- *Maintenance and repair.* Maintenance requirements should be held to a level that the average officer will do, and the firearm must be capable of repeated maintenance without damage or decrease in performance. In cases of technical malfunction, it should be easy for an officer to quickly reset the user-authorization system. A police department's armorer should be able to perform most diagnostic tests and repairs without seeking assistance from the manufacturer.

- *Adversarial compromise of technology.* It should be assumed that as soon as law enforcement agencies deploy user-authorization firearms, criminals will try to find ways to defeat the technology. It is crucial that the technology cannot be easily compromised even when a suspect has full knowledge of how the system operates. In addition, the technology should be protected against computer hackers and others who might try to disrupt the electronic systems that allow the devices to operate.

- *External devices.* Although some user-authorized firearm designs involve biometric recognition systems, other models rely on external devices, such as RFID tags, that must be worn by the user. Any external device should be as reliable, durable, and easy to use as the firearm itself. Moreover, the external device should not be uncomfortable to wear or distracting to an officer's law enforcement operations, and should not cause medical side effects to the officers.

- *Power failure.* If user-authorization technology requires batteries, they should be long-lasting and easy to recharge. A low-power indicator should warn users well before the battery runs out of power.

- *Speed of operation.* Officers have to make split second decisions of life and death. The addition of user-authorization technology should not increase the time of drawing and firing the weapon.

DHS S&T has already started the work of identifying several key issues for consideration during the development of baseline specifications. In recent months, S&T collaborated with NIJ to develop a questionnaire for law enforcement officers to determine interest in, and knowledge of, advanced gun safety technology. In March 2016, S&T sent the questionnaire to thirty law enforcement officers and administrators involved in their First Responders Resource Group, which consists of more than 150 subject-matter experts representing all major emergency response disciplines. The results of the survey confirmed that law enforcement officers possess an ongoing interest in advanced gun safety technology, but that firearm reliability remains one of the most important concerns. In addition, respondents noted that it was important that a smart gun work in both hands, be operable in all weather conditions, be comparable to current duty weapons, and have a malfunction rate no greater than current duty weapons.

Concurrently, the DHS Office for State and Local Law Enforcement contacted representatives from twelve major law enforcement associations to determine interest in advanced gun safety efforts, and these representatives indicated a desire and willingness to contribute to future discussions on baseline specifications, policy considerations, and the operational needs of law enforcement. In addition, S&T's Research and Development Partnerships Group (RDP) is identifying, locating and evaluating existing or developing technologies related to access control that can potentially be incorporated into a firearm. RDP is conducting a patent search for any patents associated with weapon safety and weapons access control.

Conclusion

This effort presents a unique opportunity for law enforcement agencies to improve their own operations and encourage the development of advanced gun safety technology. In the coming months, the Departments of Justice, Homeland Security, and Defense look forward to working with state and local law enforcement in a collaborative effort to strengthen public safety and reduce unnecessary gun violence in this country.