

EDWARD J. MARKEY  
MASSACHUSETTS

COMMITTEES:

ENVIRONMENT AND PUBLIC WORKS

FOREIGN RELATIONS

RANKING MEMBER:

SUBCOMMITTEE ON EAST ASIA, THE PACIFIC,  
AND INTERNATIONAL CYBERSECURITY POLICY

COMMERCE, SCIENCE, AND TRANSPORTATION

RANKING MEMBER:

SUBCOMMITTEE ON

SPACE, SCIENCE, AND COMPETITIVENESS

SMALL BUSINESS AND ENTREPRENEURSHIP

CHAIRMAN:

U.S. SENATE CLIMATE CHANGE TASK FORCE

## United States Senate

SUITE SD-255  
DIRKSEN BUILDING  
WASHINGTON, DC 20510-2107  
202-224-2742

975 JFK FEDERAL BUILDING  
15 NEW SUDBURY STREET  
BOSTON, MA 02203  
617-565-8519

222 MILLIKEN BOULEVARD, SUITE 312  
FALL RIVER, MA 02721  
508-677-0523

1550 MAIN STREET, 4TH FLOOR  
SPRINGFIELD, MA 01103  
413-785-4610

April 17, 2018

David B. Muhlhausen, Ph.D.  
Director  
National Institute of Justice  
810 Seventh Street, N.W.  
Washington, DC 20531

Dear Director Muhlhausen,

As the epidemic of gun violence in our nation continues unabated, I am writing regarding the efforts of the National Institute of Justice (NIJ) to promote advanced gun safety—or “smart gun”—technologies.

In April 2016, the U.S. Departments of Justice, Homeland Security, and Defense submitted a “Report to the President Outlining a Strategy to Expedite Deployment of Gun Safety Technology.”<sup>1</sup> The report considered a longstanding “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?”<sup>2</sup> To spur the development of smart gun technologies, the report proposed a partnership “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.”<sup>3</sup>

That partnership culminated in November 2016, with the issuance of a final NIJ report entitled “Baseline Specifications for Law Enforcement Service Pistols with Security Technology.”<sup>4</sup> The release of the baseline specifications followed a public notice-and-comment period, as well as the convening of several federal, state, and local law enforcement agencies and law enforcement professional associations to review and discuss draft specifications. The final NIJ report identified the law enforcement agencies’ “operational requirements for any firearms equipped with gun safety technology.”<sup>5</sup> It was intended to “make clear to private manufacturers what they expect from this technology.”<sup>6</sup>

<sup>1</sup> [https://obamawhitehouse.archives.gov/sites/default/files/docs/final\\_report-smart\\_gun\\_report.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/final_report-smart_gun_report.pdf).

<sup>2</sup> *Id.* at 1.

<sup>3</sup> *Id.* at 2.

<sup>4</sup> <https://www.ncjrs.gov/pdffiles1/nij/250377.pdf>.

<sup>5</sup> *Id.* at 1.

<sup>6</sup> *Id.*

As the lead Senate sponsor of S.1915, the Handgun Trigger Safety Act, which promotes, and eventually requires, the use of smart gun technologies, I have a particular interest in the NIJ's work on this subject. Smart gun technologies could curb the rampant number of accidental gun injuries and deaths in our country by reducing unauthorized access to dangerous weapons. For example, thus far in 2018, there have been at least 60 unintentional shootings by children—precisely the type of senseless gun violence that smart gun technologies could prevent.

Furthermore, at least two U.S.-based federally licensed firearm dealers in Maryland and California announced their intentions to include smart gun products from Armatix within their inventory for sale, but both dealers backed away from their initial commitments after experiencing harassment and death threats from zealous anti-gun safety activists.<sup>7</sup> Unfortunately, because of those death threats, Armatix was not able to successfully place its product with dealers for sale to customers.

I therefore request that, by April 30, 2018, you respond in writing to the following questions:

1. What smart gun technologies, if any, are currently on the U.S. market or are approaching market viability?
2. The April 2016 report by the Departments of Justice, Homeland Security, and Defense states that “[o]nce 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.”<sup>8</sup> Has this work occurred? If so, what research and development gaps have been identified? If this work has not occurred, why not and when will it be undertaken?
3. The April 2016 report states that “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.”<sup>9</sup> Has NIJ extended those invitations, and if so, to whom? What commitments, if any, have been made? If invited law enforcement agencies declined to make a voluntary commitment, why did they do so?
4. Apart from the invitation to make voluntary commitments to smart gun technology, is NIJ aware of any federal, state, or local law enforcement authorities purchasing firearms using advanced gun safety technologies or

---

<sup>7</sup> Michael S. Rosenwald, *Threats against Maryland gun dealer raise doubts about future of smart guns*, WASHINGTON POST (May 2, 2014), [https://www.washingtonpost.com/local/threats-against-maryland-gun-dealer-raise-doubts-about-future-of-smart-guns/2014/05/02/8a4f7482-d227-11e3-9e25-188ebe1fa93b\\_story.html?utm\\_term=.c7408d7db9a1](https://www.washingtonpost.com/local/threats-against-maryland-gun-dealer-raise-doubts-about-future-of-smart-guns/2014/05/02/8a4f7482-d227-11e3-9e25-188ebe1fa93b_story.html?utm_term=.c7408d7db9a1).

<sup>8</sup> [https://obamawhitehouse.archives.gov/sites/default/files/docs/final\\_report-smart\\_gun\\_report.pdf](https://obamawhitehouse.archives.gov/sites/default/files/docs/final_report-smart_gun_report.pdf) at 13.

<sup>9</sup> *Id.* at 12.

indicating their intent to do so? If so, please identify them and the smart gun technologies they have adopted.

5. Have any federal, state, or local law enforcement authorities implemented a pilot program for the use of gun safety technologies, as the April 2016 report contemplated?<sup>10</sup> If not, what is NIJ's understanding of why they have not? What does NIJ believe the impediments to doing so are? Is the Armatix experience an ongoing obstacle for other companies, and, if so, what can NIJ do to help overcome it?

6. The April 2016 report states that, as part of the development of the baseline specifications, "the [Bureau of Justice Assistance], 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."<sup>11</sup> How much grant funding is available? Has the NIJ, or any other federal entity of which NIJ is aware, highlighted the availability of this grant funding? If so, how? If not, why not? Have any grants been issued to support law enforcement authorities' purchase of smart gun technology? What limitations, if any, are there on the grant funding you have available to support this work?

7. The baseline specifications expressly asked for "written feedback" from those who review the document.<sup>12</sup> How many written responses did NIJ receive? Please summarize the content of those comments.

8. What level of staffing and resources is NIJ currently devoting to promoting the development of smart gun technology? Has the Attorney General or the White House provided any direction to the Office of Justice Programs or the NIJ on this issue? What type of support does NIJ need from Congress to carry out the recommendations and next steps outlined in the April 2016 report?

Thank you in advance for your attention to these requests. If you have any questions, please contact Andrew Cohen of my staff at 202-228 (b) (6)

Sincerely,



Edward J. Markey  
United States Senator

---

<sup>10</sup> *Id.* at 13.

<sup>11</sup> *Id.*

<sup>12</sup> <https://www.ncjrs.gov/pdffiles1/nij/250377.pdf> at 3.



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

JUL 20 2018

The Honorable Edward J. Markey  
United States Senate  
Washington, DC 20510

Dear Senator Markey:

This responds to your letter to the Director of the National Institute of Justice (NIJ) dated April 17, 2018, regarding advanced gun safety—or “smart gun”—technologies that may include the scanning of the owner’s fingerprint before a gun can be fired. As you are likely aware, NIJ supports state and local law enforcement through the application of science. NIJ has devoted staff and resources to activities that are likely to effectively address firearms violence in the United States, such as developing an active research and evaluation portfolio on firearms violence and gun crime.

NIJ does not provide federal grant funding to support the purchase of firearms and related equipment for law enforcement use. Regardless, NIJ is not aware of any federal, state, or local law enforcement authorities purchasing firearms using advanced gun safety technologies or indicating their intent to do so. It is NIJ’s understanding that no such firearms designed specifically for law enforcement exist.

NIJ published the Gun Safety Technology Challenge in 2015, which was halted in August 2016, during the previous Administration, after receiving a weak response, as reported in Appendix II of GAO-17-665 (<https://www.gao.gov/products/GAO-17-665>). It is the Department of Justice’s understanding, based largely on the results of the Gun Safety Technology Challenge, that the information contained in *A Review of Gun Safety Technologies*, published in June 2013, is still accurate as of May 3, 2018. It is available at <https://www.ncjrs.gov/pdffiles1/nij/242500.pdf>.

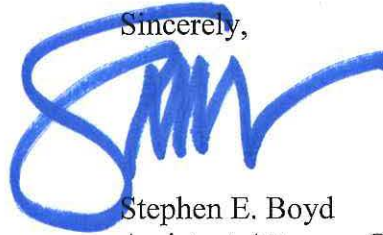
NIJ facilitated the development of the *Baseline Specifications* document, describing what law enforcement would require *at a minimum* to consider the potential use of gun safety technologies in their firearms, following the April 2016 report by the Departments of Justice, Homeland Security, and Defense. State and local law enforcement have not raised the topic of smart gun technology to NIJ as a high priority for them. Moreover, a convening of U.S. law enforcement leaders on smart guns hosted by NIJ during the development of the *Baseline Specifications* document was met with a skeptical response.

The Honorable Edward J. Markey  
Page Two

NIJ published the draft *Baseline Specifications* document via the *Federal Register* on July 15, 2016, for a 60-day comment period. It received substantive comments on the draft document from nine respondents whose comments are enclosed. NIJ issued the final *Baseline Specifications* document in November 2016.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read 'SEB', with a large, stylized loop on the left side.

Stephen E. Boyd  
Assistant Attorney General

Enclosure

## **PUBLIC COMMENTS RESPONSIVE TO FEDERAL REGISTER NOTICE 81 FR 46117**

<https://federalregister.gov/a/2016-16759>

Federal Register Notice: p. 2-3

Comments on document: p. 4-18

Comments are presented here are responsive to the request for comment on the draft document with only minimal editing to remove any identifiable information associated with the respondents.

Content in **blue** are how NIJ proposes to address a comment.

## FEDERAL REGISTER NOTICE 81 FR 46117

<https://federalregister.gov/a/2016-16759>

### Draft baseline specifications for law enforcement service pistols with security technology

**AGENCY:** National Institute of Justice, Justice.

**ACTION:** Notice and request for comments.

**SUMMARY:** The National Institute of Justice (NIJ) seeks feedback from the public on a draft document that defines generic baseline specifications for law enforcement service pistols with additional technology to enhance the security of the firearms, published here:

<http://nij.gov/topics/technology/firearms/pages/welcome.aspx>.

**DATES:** Comments must be received by 5 p.m. Eastern Time on [INSERT DATE 60 DAYS AFTER THE DATE OF PUBLICATION IN THE FEDERAL REGISTER].

**HOW TO RESPOND AND WHAT TO INCLUDE:** The draft baseline specifications document can be found here: <http://nij.gov/topics/technology/firearms/pages/welcome.aspx>. To submit comments, please send an email to [gunsafetytechnology@usdoj.gov](mailto:gunsafetytechnology@usdoj.gov). Please indicate the page number, section number, and the line number associated with each comment. Comments may also be provided as a markup of the Word document. Please provide contact information with the submission of comments. Address comments to Mark Greene, Office of Science and Technology, National Institute of Justice.

**FOR FURTHER INFORMATION CONTACT:** Mark Greene, Office of Science and Technology, National Institute of Justice, 810 7th Street NW, Washington, DC 20531; telephone number: (202) 598-9412; email address: [mark.greene2@usdoj.gov](mailto:mark.greene2@usdoj.gov).

#### SUPPLEMENTARY INFORMATION:

On April 29, 2016, the U.S. Departments of Justice (DOJ), Homeland Security (DHS), and Defense (DoD) submitted a joint report to the President outlining a strategy to expedite deployment of gun safety technology, found here: [https://www.whitehouse.gov/sites/default/files/docs/final\\_report\\_smart\\_gun\\_report.pdf](https://www.whitehouse.gov/sites/default/files/docs/final_report_smart_gun_report.pdf).

The report was published in response to Presidential Memorandum, *Promoting Smart Gun Technology*, found here: <https://www.whitehouse.gov/the-press-office/2016/01/05/memorandum-promoting-smart-gun-technology>. The report described the potential benefits of advanced gun safety technology, but noted that additional work was required before this technology is ready for widespread adoption by law enforcement agencies. In particular, the report stressed the importance of integrating this technology into a firearm's design without compromising the reliability, durability, and accuracy that officers expect from their service weapons.

To address these issues, the report called on law enforcement agencies to develop "baseline specifications," which would outline the agencies' operational requirements for any firearms equipped with gun safety technology. By developing baseline specifications, federal, state, and municipal law enforcement agencies can make clear to private manufacturers what they expect from this technology.

DOJ and DHS recently assembled a working group of experts in firearms technology to identify operational needs and prepare a draft document that defines generic baseline specifications for law enforcement service pistols with additional technology to enhance the security of firearms. The additional security specifications that may be addressed by smart gun technology are distinguished from more familiar firearm safety mechanisms. The distinction between safety and security can be nuanced, and the additional security specifications may also function as safety features under certain circumstances. However, this distinction forms the basis of the use of the different terminology.

The working group was led by NIJ and was comprised of subject matter experts from various federal law enforcement agencies. The pistols defined by this document are semi-automatic, recoil-operated, magazine-fed, striker-fired, and fire 9 mm Luger or .40 S&W ammunition. The information detailed in this document is informed in part by specifications enumerated in recent handgun solicitations by the Federal Bureau of Investigation (FBI) and Immigration of Customs Enforcement (ICE), which are publicly available on FedBizOpps (<http://www.fbo.gov>) under solicitation numbers RFP-OSCU-DSU1503 and HSCEMS-16-R-00003, respectively.

Jennifer Scherer  
Deputy Director, National Institute of Justice

## RESPONDENT 1

Our proposed additions are underlined and our proposed deletions are in ~~striketrough~~.

A.     **Section 1**           **Scope** [Begins on line 137]

**1.1** This document defines generic baseline specifications for law enforcement service pistols with additional technology to enhance the security of firearms. These specifications include features that are appropriate for law enforcement service pistols but may not be appropriate for civilian firearms. These specifications are not intended to define or otherwise limit specifications for civilian firearms incorporating security technology.

The underlined proposed addition speaks to what the document *isn't*, which is not necessary to include. The title of the document is *Draft Baseline Specifications for Law Enforcement Service Pistols with Security Technology*, which clearly indicates that it is intended for law enforcement service pistols. The document does not apply to law enforcement shotguns or patrol rifles, but that is not stated. The same logic could be applied with respect to military firearms – e.g., the specifications may not be appropriate for *military combat firearms* – however, it is not necessary to include a statement like that either.

**Comment:** As noted previously, one impetus for the NIJ's draft specifications was that, "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." In light of the ultimate goal to expand use of smart gun technologies, it is important to clarify at the outset that not all of the law enforcement specifications are appropriate for civilians. By way of example, specifications that may make sense for law enforcement, but do not make sense for civilians, include:

- Section 4.17.3 – "Pistols shall not have a magazine disconnect which prevents the firearm from firing when the magazine is removed from the pistol." This specification is not appropriate for civilians because magazine disconnects are an important safety feature helping to reduce gun accidents. In fact, they must be included in certain pistols sold to consumers in California, in accordance with the Unsafe Handgun Act.<sup>3</sup>
- Section 4.18.4 – "The security device shall not inhibit the operator from firing...with and without gloves...." Since civilians may not want or need to wear gloves when operating guns, a more useful specification for civilians would allow for fingerprint recognition, even if this technology could not work with gloves.
- Section 4.18.6 – "The security device shall not increase the time required by the operator to grasp, draw from a holster, and fire the pistol as a pistol of the same design that is not equipped with a security device." Since civilians may not keep their guns in a holster, a more useful specification for civilians could define the maximum amount of time from first contact to recognition of an authorized user to firearm enablement.
- Section 4.18.7 – "The security device shall not emit audible sounds or visible signals." Section 4.18.11 further states that low power shall be indicated "covertly." For civilians, it would be

---

<sup>3</sup> See Cal. Penal Code §§ 32000(a), 31910, 16900.

safer for a low battery or low power source to be indicated by audible sounds and visible signals, to alert the consumer to recharge the battery or other power source.

Our proposed revision to Section 1.1 would clarify that the NIJ's specifications for law enforcement are not intended to limit the availability of features described above in civilian firearms incorporating smart gun technology. Doing so will also make clear that the "federal government seeks to expand, not constrict, consumers' choices when deciding what firearm to purchase."

The above commentary discusses the justification for the proposed addition. Addressing civilian firearms is outside of the scope of this document.

**Section 5.1 Reliability** [begins on line 817]

**5.1.1** ~~Pistols shall have a mean overall malfunction or failure rate of no greater than 1 in 2,000, or shall exhibit a mean rounds between failure of no less than 2,000.~~  
Pistols shall fire 2,000 rounds of ammunition with no more than one malfunction, excluding malfunctions that are traceable to ammunition that fails to detonate or operator error.

**5.1.2** ~~Pistols shall exhibit zero malfunctions or failures related to reliability that are attributable to the security device after 2,000 presentations from the holster and firing 10,000 rounds per pistol.~~

**5.1.3** ~~Pistols shall exhibit zero malfunctions or failures related to reliability that are attributable to the security device~~ a mean overall malfunction or failure rate of no greater than 1 in 2,000, excluding malfunctions or failures that are traceable to ammunition that fails to detonate or operator error, after environmental exposures subject to the MIL-STD-810G laboratory test methods listed below ...

Section 5 will be reviewed for clarity. Sections 5.1.1 and 5.1.3 specify the reliability requirements in terms of statistical measures. The suggested revision in 5.1.1 changes the meaning a bit. Specifying a malfunction or failure rate, or mean round between failure, does not actually specify the firearm sample size or total rounds to be fired during testing, which likely requires many more than 2,000 rounds and more than one firearm. Further discussion through a consensus-based process is needed to determine the sample size and number of rounds to be tested. Section 5.1.2 is seeking to specify testing a pistol through its expected life cycle, which will be moved to the durability requirements. It also includes the use case of drawing and firing from a holster, which is will remain with revised language.

Section 5 has been revised and expanded into the following sections:

- 5.1 Accuracy and dispersion**
- 5.2 Reliability and durability**
- 5.3 Environmental exposure**
- 5.4 Mechanical shock**

These sections elaborate and clarify the performance requirements and testing to be performed on firearms that shall meet the specifications.

**Comment:** The draft specifications provide for an overall malfunction or failure rate of 1 in 2,000, but further specify that no malfunctions or failures can be attributable to the security device, including after environmental testing. This potentially sets an impossibly high standard, under which the security device must always operate perfectly, even though it is contemplated that the rest of the pistol may exhibit a failure or malfunction rate of 1 in 2,000 and still be deemed reliable. We propose revising this standard to provide that the security device must perform equally as reliably as the rest of the pistol, which sets a high, but fair, bar for reliability. Moreover, as currently drafted, the 1/2,000 failure rate is very stringent. Other NIJ specifications for police firearms have allowed significantly higher failure rates,<sup>4</sup> as does California's testing process under the Unsafe Handgun Act.<sup>5</sup>

We also propose clarifying that the 1 in 2,000 failure or malfunction rate excludes failures or malfunctions that are attributable to ammunition that fails to detonate or operator error, in order to precisely define what constitutes a failure or malfunction, and to match the reliability standards outlined in footnotes 4 and 5.

In addition, we propose eliminating the requirement that 10,000 rounds per pistol be fired to test the security device. The reliability standards cited in footnotes 4 and 5 describe a testing process during which only 600 rounds are fired. In light of these precedents, a 2,000 round test appears to be more than adequate to determine the reliability of a pistol and its security device.

An average malfunction rate of 1 in 2,000 is very achievable with pistols engineered and manufactured for law enforcement today. The 1999 NIJ standard is also a minimum performance standards that is due for revision.

The above commentary discusses the justification for the proposed revision. Please see the above for the revisions made. The NIJ standard referenced is due for updating in the near future as many pistols for law enforcement greatly exceed the minimum performance requirements in NIJ 0112.03 Rev A today.

**B. Section 4.18 Security Devices** [begins on line 598]

**4.18.1** Pistols shall have an integrated "lock-out" security device as a permanent part of the pistol that disables the firing control system except when in the control of authorized individuals.

**4.18.2** The security device ~~may shall be understood to include~~ any externally worn items, such as rings, wristbands, or tokens that perform functions associated with the security device. The security device may also include a permanent

<sup>4</sup> See National Institute of Justice, *Autoloading Pistols for Police Officers*, NIJ Standard-0112.03 Revision A at 7 (July 1999), available at <https://www.justnet.org/pdf/NIJSTD011203REVA.pdf> ("When tested in accordance with Section 5.6.1, the pistol shall fire 600 rounds of ammunition with no structural or mechanical failures and no more than five malfunctions.").

<sup>5</sup> Cal. Penal Code § 31905(b)(1) ("The laboratory shall fire 600 rounds from each gun..."); *id.* § 31905(c) ("A handgun shall pass [the 600 rounds] test if each of the three test guns meets both of the following: (1) Fires the first 20 rounds without a malfunction that is not due to ammunition that fails to detonate. (2) Fires the full 600 rounds with no more than six malfunctions that are not due to ammunition that fails to detonate and without any crack or breakage of an operating part of the handgun that increases the risk of injury to the user.").

programmable biometric feature as part of its original manufacture that performs those functions.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately, however the respondent may have misunderstood 4.18.2. Many smart gun prototypes over the years have included externally worn devices as a part of the firearm system. Therefore, any externally worn device or token shall be included as a part of any firearm system that attempts to meet the specifications. Explicitly stating this provides clarity that externally worn devices should be included in all testing.

Furthermore, the requirements in 4.18 are designed to be technologically agnostic so as not to include or exclude any particular technology; rather, any viable technological approach to meet the requirements is permissible. Calling out that a biometric feature may be included is not necessary. Various technologies that could be used are discussed in the *Report to the President Outlining a Strategy to Expedite Deployment of Gun Safety Technology* from April 2016 and the NIJ report from June 2013. However, technologies that may meet the requirements are not limited to what has been discussed in these reports.

**Comment:** In section 4.18.2, we propose two edits: (i) replacing “shall be understood” with “may,” in order to clarify that while the security device can include an externally worn item, it does not necessarily have to include such an item; and (ii) adding language to ensure that biometric recognition is specifically identified as a possible component of a security device.

The above commentary discusses the justification for the proposed addition.

C. New Section 4.19 [to begin on line 642]

4.19 Optional safety features. Pistols may include other safety features, such as: (1) the capability to send information about a pistol's location to authorized individuals; (2) a QR code that would enable a recovered firearm to be uniquely identified; (3) a display that indicates if a pistol is loaded and how many rounds it contains; (4) “sleep” or “off” modes that render a pistol inoperable until re-activated by an authorized user; (5) a “black box” feature that sends information to authorized individuals about rounds fired and/or sends a distress signal with location information when rounds are fired.

The baseline specifications document is designed to be a consensus-based document. However, given the timeline for the development of the document, there is not sufficient time to achieve consensus on whether these features should be included, even as optional features. The document does not preclude firearms from having features above and beyond what is specified.

**Comment:** We propose adding a new section 4.19 entitled “Optional safety features.” The section would identify optional safety features a manufacturer could develop and incorporate into a law enforcement service pistol. Each feature would improve the ease with which law enforcement pistols may be safely handled and recovered if lost or stolen. Below, we explain the rationale for including each of these four optional features.

Electronic recovery. Law enforcement pistols could include a computer chip that would allow a gun to

be tracked and retrieved if it is lost or stolen. Additional applications of this promising technology were discussed in the April 2016 Report, which noted that sophisticated electronic recovery systems “can collect additional information about a gun’s use,” such as whether a gun has been removed from the holster or discharged, and notify dispatchers when an officer needs back-up.

Electronic tracing enabled. Law enforcement pistols could include a QR or matrix bar code that is affixed to each firearm that would enable a recovered pistol to be uniquely identified. This technology would improve the ability of law enforcement officers to trace stolen firearms, possibly through use of a smart phone application. For domestic manufactured firearms, the code could include information like serial number, manufacturer, caliber, and model; for foreign manufactured firearms, the code could also include country of origin and importer.

Load indicator. Law enforcement pistols could incorporate a load indicator, which visually indicates whether a pistol is loaded and how many rounds it contains.<sup>6</sup> Although cars tell drivers how much gas is left in the tank, and phones display how much battery life remains, there is currently no way to tell at a glance how many rounds remain in the chamber of a gun. For the untrained or distracted user, the lack of certainty over the number of remaining rounds can lead to unintended discharges, injury, or death. For police officers, a load indicator could improve officer safety during protracted gun fights or other deadly situations where counting rounds is difficult.

Sleep mode. Loading and unloading a firearm is not without risk of accidental discharge. Indeed, many police departments require officers to aim into a bullet trap as they unload their guns, but officers may not have access to such devices in their homes, or when entering secure facilities where loaded guns are not permitted. Smart gun technology could give authorized users a way to safely and easily “turn off” a gun or put it in sleep mode when going home or entering secure locations like jails and courthouses.

“Black box.” We are all familiar with the importance of the flight recorder, often called a “black box,” that delivers information about airplane accidents. Smart gun technology could similarly aid investigators examining crimes or police involved shootings. A black box feature in a law enforcement pistol could collect information such as the number of rounds fired, the timing of fire, or the direction of fire, in order to either confirm or challenge eyewitness testimony. A black box feature could also be programmed to send a distress signal if an officer’s gun is fired or removed from the holster. It could additionally be programmed to turn on an officer’s body camera; obtaining camera footage automatically when a gun is unholstered can help law enforcement investigate crimes and shootings, including in circumstances where an officer is killed on duty. Black box technologies like these already exist in Tasers carried by some police departments.<sup>7</sup>

The above commentary discusses the justification for the proposed addition.

---

<sup>6</sup> As part of the Unsafe Handgun Act, California requires that certain pistols include either a magazine disconnect or a “chamber load indicator,” a device that plainly indicates a cartridge is in the firing chamber. See Cal. Penal Code §§ 31910(b)(4), 16380.

<sup>7</sup> See, e.g., Lily Hay Newman, *LAPD Body Cams Will Automatically Start Recording When Police Use Tasers*, FUTURE TENSE (Jan. 8, 2015, 1:58 PM), [http://www.slate.com/blogs/future\\_tense/2015/01/08/the\\_lapd\\_is\\_ordering\\_more\\_than\\_3\\_000\\_smart\\_tasers\\_that\\_will\\_activate\\_body.html](http://www.slate.com/blogs/future_tense/2015/01/08/the_lapd_is_ordering_more_than_3_000_smart_tasers_that_will_activate_body.html).

## RESPONDENT 2

1. Section 4 (Baseline Specifications) Line numbers 228-812: The firearm requirements will limit technical development of solutions for security technology.

This is the opinion of the respondent.

- General comment: The specifications listed in Section 4 will hamper research and development. We strongly advise against limiting the universe of firearms that will qualify for consideration. Such limitation will stifle technological development and advancement and prevent discovery of better security solutions than those identified in the Draft Specifications.

This is the opinion of the respondent.

- The pistol requirements are very similar to recent FBI and DHS solicitations for new duty pistols. Because the requirements are very specific, it would appear that the Government only wishes to have the same or a very similar pistol to a recent award, but enhanced with smart gun technology. There were a limited number of firearm manufacturers who had product solutions to support the FBI requirements. In order to encourage participation on the part of firearm manufacturers, we recommend NIJ relax the requirements not strictly directed at the security system.

This is the opinion of the respondent. The FBI and DHS solicitations were used as a foundation for the specifications as they are major procurement actions for Federal law enforcement pistols and have achieved a level of consensus on their content. Market research by the FBI indicated several existing makes and models that fall within the form factor range. This document represents law enforcement requirements for a pistol and there will be some constraints on the form factor as a result. The range of form factor is also not unusual for pistols. Any firearms manufacturer who wishes to meet these requirements should be able to do so.

- § 4.1 Action (Lines 230-234): specifies that pistols shall be striker-fired and shall not have a hammer, either internal or external. As reported in "Report to the President Outlining a Strategy to Expedite Deployment of Gun Safety Technology", existing smart gun technologies thus far have had limited success and reliability with traditional firing mechanisms. Specifying which type of operation a smart pistol must have will limit available solutions to today's technology and rule out future advances in primer ignition systems which could function more reliably for the intended purpose.

This is the opinion of the respondent.

- § 4.3 Barrel (Lines 241-261): The requirement for the barrel length and minimum capacity for Class I and Class II pistols will potentially rule out manufacturers who do not currently have pistol products which fit into these defined classes. It is recommended that this be relaxed and include "threshold" and "objective" capacity and barrel length requirements which would allow a wider range of "host weapons" to satisfy the security devices requirements in §4.18.

Market research by the FBI indicated several existing makes and models that fall within the form factor range. This document represents law enforcement requirements for a pistol and there will be

some constraints on the form factor as a result. The range of form factor is also not unusual for pistols. Any firearms manufacturer who wishes to meet these requirements should be able to do so.

2. Section 4.18 (Security Devices) Lines 598 -640: Some requirements related to the security system seem to be contradictory or mutually exclusive.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately. However, as this document represents law enforcement operational requirements in a technologically agnostic way, the burden is not on law enforcement to write these requirements to accommodate technology. Rather, the burden is on industry to find a technological means to meet the requirements.

- § 4.18.2 (Line 604): this section specifies the security device shall be understood to be any externally worn items that perform functions associated with the security device. As this requirement favors a system with externally worn items by excluding technologies not dependent on an external device, this will stifle research and development and improvement of security systems.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately, however the respondent may have misunderstood 4.18.2. Many smart gun prototypes over the years have included externally worn devices as a part of the firearm system. Therefore, any externally worn device or token shall be included as a part of any firearm system that attempts to meet the specifications. Explicitly stating this provides clarity that externally worn devices should be included in all testing.

- § 4.18. 7 (Line 621): states that the pistol shall not emit audible sounds or visible signals. The requirements of §4.18.9 and §4.18.11 require covert indication of the pistol's status. These three requirements appear to be contradictory. Without visual or sound cues, few options are available for an operator to "sense" the status of the pistol. We recommend revising this section to allow for subtle signals communicated either audibly or visually. A similar parallel system is a loaded chamber indicator on a handgun, which is both visual and tactile.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately, however the requirements do not exclude tactile feedback or visible indicators on the gun that are covert or known only to the officer. Audible and visible signals may be distracting to the officer or may compromise a covert or hidden position, both of which could negatively impact officer safety.

- § 4.18.12 (Line 636): this section states that if the security device malfunctions the weapon should default to a firing state. Consequently, with a battery-operated security system, the firearm will revert to a firing state if the battery runs down or is removed by an unauthorized person. Presumably, the working group drafted this provision to protect law enforcement against injury or death due to an inoperable firearm. We believe this highlights the fact that the security technology identified in the Draft Specifications is inherently flawed and therefore not a viable requirement because of the danger to law enforcement in a real-world scenario. The fact that any battery-operated security system will be operationally accessible to any user is contrary to the intent of the "smart gun" program.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately, however law enforcement operations demand that officer safety receives the highest priority. The respondent's

comments are speculative regarding the use of a battery-operated security systems, however it's not clear that the respondent's comment is discussing a malfunction issue, a preventative/scheduled maintenance issue, a design issue, or some combination. For example, neglect of preventative/scheduled maintenance that may lead to a firearm not functioning properly will be an issue for any firearm, not just a smart gun. There is probably never a perfect way to deal with a possible malfunction, however officer safety must be the priority.

- § 4.18.13 (Line 639): this section states that the security device should be easy for an operator to quickly reset or disengage if there is a malfunction. Based on the requirement of § 4.18.12, this would mean that a gun which could not be unlocked by the operator could easily be returned to a firing (default non-secure) state. If it is easy to return the gun to a firing state, the security system is defeated easily.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately, however law enforcement operations demand that officer safety receives the highest priority. There is probably never a perfect way to deal with a possible malfunction, however officer safety must be the priority.

- The three technologies referenced in the "Report to the President Outlining a Strategy to Expedite Deployment of Gun Safety Technology" - Radio Frequency Identification (RFID), Dynamic Grip Recognition (DGR) and fingerprint biometrics - each have limitations or drawbacks in comparison to the requirements outlined in § 4.18. None of these technologies have clear mitigating development paths which will culminate in successfully meeting the draft requirements. Consequently, the continued pursuit of these technologies will ultimately result in the inability to gain confidence in the user community.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately. However, as this document represents law enforcement operational requirements in a technologically agnostic way, the burden is not on law enforcement to write these requirements to accommodate technology. Rather, the burden is on industry to find a technological means to meet the requirements.

The specific drawbacks that are identified on these technologies:

- (1) Radio Frequency Identification (RFID)
  - a. The system is dependent upon a secondary device which must be present to allow the firearm to be operable - a ring, a wrist-band, a glove, etc. There are legitimate real-life situations where such a device would not be present (e.g. weak arm shooting due to disablement of the strong arm). While some situations can be mitigated through the use of repetitive equipment (i.e. putting a wrist-band on both wrists, instead of just one), this simply multiplies the potential for something to go wrong or for the officer to forget equipment.
  - b. RFID systems make use of the electromagnetic spectrum, as with Wi-Fi networks or cellphones. The draft baseline requirements call out a need to equip countermeasure detection technology, which builds more and more complication into the circuitry. The result of added complication in a system is that more things can go wrong, which is opposite from the desired direction

for a firearm, which should be as simple as possible. This relates to the draft requirement in §4.18.8.

- c. Electromagnetic shielding may be the best mitigation against interference, which causes additional complications and risks to reliability. Again, this relates to the draft requirement in §4.18.8.
- d. With the right equipment, a person can read the RFID signal and recreate it with their own equipment. Once the system is defeated, products can be made available on the black market which allow for the firearm to be used by criminals. This defeats some of the purpose of having the system to begin with – allowing criminals to defeat the system.

(2) Dynamic Grip Recognition (DGR)

- a. The draft requirement in §4.18.3 states the security device should be capable of being set to allow one or more operators to use the pistol. The ability for multiple officers to access and use the same firearm with DGR is questionable. It is unclear if it is feasible to program the system to allow multiple users without also making it usable for those desired to be locked out of the system. It is theorized that the acceptance rate of the system would need to be relaxed to a point where too many undesired users would be able to use the system. This compromises the purpose of the security system, and violates §4.18.1, which requires that the system only work in the control of authorized users.
- b. The draft requirement of §5.1.3 states pistols shall exhibit zero malfunctions or failures related to reliability that are attributable to the security system. Environmental robustness must be mitigated. High and low temperatures, contaminants, as well as moisture are all high risk concerns that might affect grip pattern, and cause a false rejection. As with accepting multiple users, the most likely mitigation would be to relax the acceptance rate of the system. This would further compromise the security system, again in violation of §4.18.1.
- c. An officer's grip may change as the officer's firing technique evolves, or if the officer encounters a physical transformation of the hand (e.g. due to an injury). This may either render the firearm to be non-functional, or else require an expansion of the acceptance tolerance which renders the system to be compromised. Again, this would be a violation of §4.18.1.

(3) Fingerprint Biometrics

- a. Gloves are not compatible with fingerprint biometrics. This violates the draft requirement in §4.18.4.
- b. Fingerprint recognition technology cannot be proven to be sufficiently reliable, both due to environmental and tactile situational variations. If the finger pad is wet or soiled, for instance, the finger pad must first be wiped clean prior to using.

- c. The additional step of ensuring that the finger is properly placed onto a fingerprint biometric sensor adds precious time which can cost the user his or her Life. This also violates the draft requirement in §4.18.6, which states that the security device shall not increase the time required by the operator to grasp, draw and fire the pistol.
- d. The draft requirement in §5.1.3 states pistols shall exhibit zero malfunctions or failures related to reliability that are attributable to the security system. Environmental robustness must be mitigated. High and low temperatures, contaminants, as well as moisture are all high risk concerns that might affect electronic function or affect grip pattern and have a negative effect.

The above discussion of the three technologies offers perspectives on the perceived problems with how those technologies would be challenged to meet different aspects of the requirements document.

### RESPONDENT 3

#### A. "Basic Requirements"

- We note that an appropriate mechanical gun lock is to accompany each pistol. This device can provide the required security technology without the disadvantage of electromechanical or battery-powered devices as further discussed below.
- We also note that a basic requirement is to omit magazine safeties, even though such a device can render the pistol unable to fire by the touch of a button to drop the magazine.
- In your lengthy description of slide stop requirements, you state that it must
  - be operable using a single finger or thumb.
  - be articulable during one-handed use while maintaining a positive grip on the pistol.
  - be easily manipulated by both right and left handed operators
  - not be inadvertently engaged or over-ridden during normal use.
  - prevent inadvertent functioning by the operator during one-handed or two-handed thumbs forward grip purchases, and
  - be provided in two sizes to fit different hands.

We submit that all of these requirements should apply with equal force to any security device, which are at least as important as the slide stop.

- External thumb and grip safeties and decocking levers are not permitted, yet they all help provide additional security from accidental or unauthorized uses of the pistol.
- The grips are to be useable when wet or dry, be fully ambidextrous, allow for the accommodation of at least three different hand sizes without tools, and not be held in place by the use of screws.

We believe that such specifications should apply equally to security devices, which are at least as

important as the grips.

- The sights must successfully complete 20,000 endurance firing cycles, cannot snag in a holster, not be damaged by available solvents and lubricants, and have a minimum service life of ten years.

We believe these specifications should apply equally to security devices, which are at least as important as the sights.

Section 4 will be reviewed to ensure that the requirements are stated appropriately.

B. "Durability"

- Resistance to rust as set forth in the Draft Specifications should also apply to the security device, as should resistance to salt water corrosion.
- The requirement of having no gouges, sharp edges, or rough areas to snag on holsters, clothing, or which can cause injury to the operator, should also apply to the security device.
- The security device as well as the pistol should be compatible with various commercially available holsters.
- The requirements that the average officer can maintain the pistol, which must be capable of repeated maintenance without damage or decrease in performance, must also apply to the security device.
- The requirement that no tools be needed to field strip the pistol should not be compromised by the security device, especially if immediate action is required to restore the pistol to its firing mode.
- The requirement that a unit armorer should be able to diagnose and repair the pistol without seeking assistance from the manufacturer should apply to the security device as well.
- We believe that the 2,000 mean rounds between failure and Mil. Std. 810G tests (high temperature, low temperature, fluids, rain, salt fog, sand, dust, immersion in a pool, lake, or river, humidity, sweat, electronic interference, and the SAAMI drop tests) are all appropriate tests for the security device.
- And any rings, wristbands, watches, or tokens needed to operate the security device must also pass the same durability tests.

The requirements discussed above, which are found in the document, apply to the pistol and all of its parts or components. For example, when the requirements state "pistols shall...", that includes all parts of the pistol, including security devices.

C. "Security Devices"

- The stated inconvenience is that the security device "disables the firing system except when in control of the authorized user."

This is not accurate as stated. The described security device can disable the firing system except when any user is in control of an enabling device, which could be anyone in possession of same, whether or not that person is "the authorized user."

- The security device “includes external items such as rings, wristbands or tokens.”

So any possessor of these external items or any other item which can disable the security device, such as a magnet or RFID signal, becomes in effect “an authorized user.”

- The security device must be programmable to allow others to operate the firearm, but it must not permit other persons with ability to program it to disable its functioning by the primary user or users.
- The requirement that the security device shall not inhibit firing from either hand, with either a one-handed or two-handed grip, with or without gloves, and in any orientation, is a good one. However, it would appear to rule out any biometric devices requiring direct contact with the pistol such as, fingerprint or grip recognition technology.
- The security device “shall not alter the normal operation of grasping, drawing or firing the pistol,” nor shall it “increase the time to operate the pistol.”
- Again, this would seem to rule out security devices which require precise placement or orientation of an authorized user’s hand, especially in time of stress or injury.
- The requirement that the device not emit “audible or visible signals” would rule out a low battery indication, yet other conflicting requirements state that the device must “covertly” indicate when the pistol is ready to fire or its battery has a low power condition.
- The requirement that if the security device is suspect to electromagnetic interference it must be equipped with a countermeasure to permit firing when an attempt to block firing is detected, will seemingly add even more complexity and require yet another indicator to the user.
- It should be noted that any magnetically-opened device can be defeated by the application of commonly available magnets, such as refrigerator magnets.
- If the security device uses batteries, they must be rechargeable and replaceable.
- Here is the single biggest problem with any battery powered device... when the battery fails, the status of the security mechanism will change from what the authorized user has set and expects. Either a firearm relying upon a non-functioning security device to be in a “safe” mode from unauthorized use will unexpectedly be able to fire; or a firearm relying upon a read battery to be made ready to “fire” will be unable to be used by the unauthorized user. Neither is an acceptable option for firearms designers because either failure mode can cost lives -- either the pistol on its security mechanism will unexpectedly fail to operate as set, and intended by the authorized user.
- The draft specification seems to anticipate this Hobson’s choice by requiring that the default mode when the battery fails is the fire mode. This is deceptive and hazardous to the user and to the public who will rely upon such devices to prevent unauthorized use of a pistol so equipped, only to discover that at an unknown later date, the security mechanism is inoperative and the pistol will fire.
- Finally, the security device is supposed to be easy to reset or disengage if it malfunctions. Again, the authorized user will be spending precious time diagnosing and disengaging the security device if it malfunctions, even though the intent is “to activate a blocking mechanism in a seamless process that is designed to take less time than handling and firing a conventional gun. And if it is readily disengagable because of a hidden malfunction, it is not “security.” It is a trap with the illusion of security.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately.

## RESPONDENT 4

**Specific comments in sequence to the report:** "Draft Baseline Specifications for Law Enforcement Service 21 Pistols with Security Technology" **Comments in red.**

We can start at 4.18 "Security Devices" as the rest is boiler-plate and I'm generally familiar with the other specs. Those sections I do not have comments on, I will ignore.

623: 4.18.8 If the security device may be susceptible to electromagnetic interference, either intentional or unintentional, the device shall be equipped with countermeasure detection technology that permits the operator to fire the gun when an attempt to block the authorization process is detected.

*We feel if someone is going to aim and shoot a jamming signal at an officer, they could just as well aim any other weapon. We're talking such a remote possibility as to be insignificant. Yet inclusion of this requirement could eliminate this technology from saving lives.*

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately.

636: 14.18.12 If the security device malfunctions, it shall default to a state to allow the pistol to fire.

*We can design guns to comply with this, yet it will raise cost and have other potential negative ramifications. If the Smart System is as reliable as a regular firearm why should it fail fire? Last time I saw a broken firing pin or spring in a gun, it failed "fail". I guess you guys are buying guns even I don't know about!*

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately.

815: 5. PERFORMANCE REQUIREMENTS

822: 5.1.2 Pistols shall exhibit zero malfunctions or failures related to reliability that are attributable to the security device after 2,000 presentations from the holster and firing 10,000 rounds per pistol. *Yet it is OK for the gun to fail 1 in 2,000 in 5.1.1?*

5.1.3: Pistols shall exhibit zero malfunctions or failures related to reliability that are 826 attributable to the security device after environmental exposures subject to the MIL-STD-827 810G laboratory test methods listed below:

- High Temperature: 501.5 830
- Low Temperature: 502.5 832
- Contamination by Fluids: 504.1 834
- Rain: 506.5 836
- Salt Fog: 509.5 838
- Sand and Dust: 510.5 840
- Immersion: 512.5

*We could meet and has previously met certain of these requirements. Those most important we would spend more time on. Salt Fog in a courthouse? Probably not. Salt Fog for USCG? Definitely.*

Section 5 will be reviewed for clarity. Sections 5.1.1 and 5.1.3 specify the reliability requirements in terms of statistical measures. The suggested revision in 5.1.1 changes the meaning a bit. Specifying a malfunction or failure rate, or mean round between failure, does not actually specify the firearm sample size or total rounds to be fired during testing, which likely requires many more than 2,000 rounds and more than one firearm. Further discussion through a consensus-based process is needed to determine the sample size and number of rounds to be tested. Section 5.1.2 is seeking to specify testing a pistol through its expected life cycle, which will be moved to the durability requirements. It also includes the use case of drawing and firing from a holster, which is will remain with revised language.

Section 5 has been revised and expanded into the following sections:

- 5.1 Accuracy and dispersion
- 5.2 Reliability and durability
- 5.3 Environmental exposure
- 5.4 Mechanical shock

These sections elaborate and clarify the performance requirements and testing to be performed on firearms that shall meet the specifications.

## RESPONDENT 5

Comments are relative to section 4.18 "Security Devices" that starts on page 14 of the Draft Baseline Specifications document.

Pistols should be connected to and controlled via cloud based network that would enable or disable key firing system components depending on the needs and requirements of the controlling organization.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately. The baseline specifications document is a consensus-based document, but given the timeline for the development of the document, there is not sufficient time to achieve consensus on whether these features should be included, even as optional features. However, the document does not preclude firearms from having features above and beyond what is specified.

### Additional comments and recommended enhancements to section 4.18 "Security Devices:"

- Pistols shall be infused with smart components and technologies such as a battery, SIM card, Wi-Fi and Bluetooth capability, antennas, and electromechanical firing control enablers.
- Pistols should be "network controllable" such that it would be able to receive inputs and controls from a variety of sources and controlled according to the needs and desires of the controlling agency.

- Pistols could be permanently or semi-permanently disabled from a controlling device on the network. One or more parts of the smart-gun could be selectively broken or deformed such that the weapon would only become fireable again with considerable time, work, or difficulty. Disableable replacement parts would be tightly controlled.
- Pistols shall be enabled via Bluetooth pairing with a smart phone via short range (Class 3) pairing such that the pistol will fire if located within one meter of the smart phone but become inoperable if taken beyond one meter of the smart phone (in case a pistol is taken from an officer) (*proximity enablement*).
- Pistols will have the capability (via the controlling agency) to be enabled or disabled based on *time of day and or date*.
- Pistols will have the capability to be enabled or disabled based on *geographic location*.
- Pistols will have the capability to be enabled based on close *proximity to an enablement device* for use in *shooting ranges for training purposes*.
- Pistols will be a part of a cloud based system that will allow law enforcement organizations *to remotely control large groups of weapons, individually or collectively*. Such control will be available through a combination of any suitable communications network, including satellite, cellular, Wi-Fi or the like. Such a control system would include capabilities to lock, unlock, or disable one or more pistols.
- Pistols will be configured to use passive Wi-Fi which consumes 1,000 times less power than typical Wi-Fi portals.
- Pistols will use backscattering charging technology to charge the internal battery. This technology enables devices to selectively reflect incoming radio waves to construct a new signal, absorbing energy from ambient Wi-Fi signals to trickle charge the internal battery.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately. The baseline specifications document is a consensus-based document, but given the timeline for the development of the document, there is not sufficient time to achieve consensus on whether these features should be included, even as optional features. However, the document does not preclude firearms from having features above and beyond what is specified.

## RESPONDENT 6

From pages 14 and 15 (emphasis mine):

**4.18.6** The security device **shall not increase the time required** by the operator to grasp, draw from a holster, and fire the pistol as a pistol of the same design that is not equipped with the security device.

## RESPONDENT 7

Section 5.1.2 of the Baseline Specifications for Law Enforcement Pistol Security Technology concerning the durability of the pistol security technology are grossly unrealistic. Polymer service pistols have service lives far in excess of 10,000 rounds when properly maintained. Security systems will by their very nature be expensive components that will make it very difficult for law enforcement agencies to replace in times of high federal deficits and decreasing resources. Therefore, the durability requirement in Section 5.1.2 should be at least 10,000 presentations and 40,000 rounds to include practice presentations under controlled conditions and rounds fired in training as well as qualification.

Section 5.1.2 seeks to specify testing a pistol through its expected life cycle, which includes a total number of rounds and the use case of drawing and firing from a holster.

## RESPONDENT 8

My comments regard page 14, section 4.18.8 from lines 623-626. I request that the following language be added to the end of the paragraph on line 626 "This countermeasure detection technology shall be inherent to the design of any and all firearms with this security technology and not be just exclusive to service pistol models prepared for and supplied to law enforcement. Further, no firearms, including service pistols, with this security technology shall have any ability to be remotely geo-located or remotely rendered inoperable with a 'kill-switch or other device.' "

The baseline specifications document is a consensus-based document, but given the timeline for the development of the document, there is not sufficient time to achieve consensus on whether these features should be included, even as optional features. However, the document does not preclude firearms from having features above and beyond what is specified.

## RESPONDENT 9

The document was well constructed and informative from the view of creating an entirely new firearm. With that being said, I would like to introduce and explore a slightly different direction.

I would like to see Law Enforcement and industry co-create a "retrofit" kit for already existing firearms. As I am sure you already know, due to increased operating budgets, the cost of a issuing new firearms could be a financial burden to many Departments. However, if a reduced cost, "retrofit" solution were available, Departments may have an easier time absorbing the cost.

In my opinion, the ideal retrofit kit would incorporate the following attributes:

- **Reliable** (Should function reliably. 99.99% or 99.999% of the time. Realistically, no device operates 100% of the time)
- **Cost Effective** (Retrofit solution should not cost more than the original price of the firearm)
- **Easy/Quick to Install and Maintain** (The fewer steps to configure and maintain, the better.)
- **Incorporate Event Tracking** (Date/Time, Location, Sound/Video, Biometric logging, etc.)

**4.18.9** The security device shall covertly indicate **when the pistol is ready to fire**.

**4.18.12** If the security device malfunctions, it shall default to a state to allow the pistol to fire.

The three items cited above are of grave concern to me.

Although **4.18.16** specifies that the security device must not increase the time required to grasp, draw, and fire, anything added to this process must *necessarily* lengthen the time it takes to fire the weapon. A law enforcement officer or agent suddenly confronted by an immediate, deadly threat from an armed assailant must know his weapon will fire as soon as he pulls the trigger. Anything less than instantaneous, flawless recognition would be deadly. The process of drawing, establishing a grip, aiming in, and firing can be done by a proficient LEO in merely one or two seconds; and sometimes all an LEO has are seconds to fire before an assailant fires on him.

The respondent speculates that the addition of a security device will lengthen the time to grasp, draw from a holster, and fire the pistol, however that is not what the requirement states. The requirement already addresses the concern of the respondent. The burden is not on law enforcement to write these requirements to accommodate technology. Rather, the burden is on industry to find a technological means to meet the requirements.

Item **4.18.9** specifies that there would be an indicator which shows the officer the weapon is ready to fire. Having to be mindful of an indicator is a needless, time-wasting distraction. When an officer is confronted with an immediate, deadly threat, he does not look at his weapon at **any** time during the process of drawing and firing other than to look through the sights. Checking an indicator only increases the time it takes to address the threat, thereby increasing the danger to the officer.

The respondent speculates that the covert indicator will be visual, which is not what is stated. We agree that audible and visible signals may be distracting to the officer or may compromise a covert or hidden position, both of which could negatively impact officer safety, which is why the manner of indication is agnostic. The burden is not on law enforcement to write these requirements to accommodate technology. Rather, the burden is on industry to find a technological means to meet the requirements.

And finally, item **4.18.12** recognizes the fact that this technology can never work 100% of the time. Aside from that, the fact that the weapon would then “default to a state that would allow it to fire” would *itself* have to occur instantly and flawlessly.

Section 4.18 will be reviewed to ensure that the requirements are stated appropriately. Officer safety must be the priority which is reflected in this requirement. The reliability requirements in Section 5.1 sets the reliability levels of the pistol overall, which includes malfunctions that could arise from all features of the firearm, at a rigorous but achievable level for today’s law enforcement pistols to ensure high performance and low failure. Malfunctions from security devices are included in that overall malfunction rate. In addition, security devices must meet the overall durability requirements in 5.2 as well. These requirements ensure that the incidence of malfunctions will already be very low.

- **Ability to operate the firearm by multiple users** (i.e. If Officer A needs to use Officer B's firearm in an active situation)
- **Ability to operate the solution in harsh environments** (Extreme cold/heat, elevated moisture and particulate levels)
- **Avoid substantially changing the grip style of the firearm**

The document does not preclude the development of a retrofit kit. However, the retrofitted firearm would still have to meet all the requirements in the specifications.